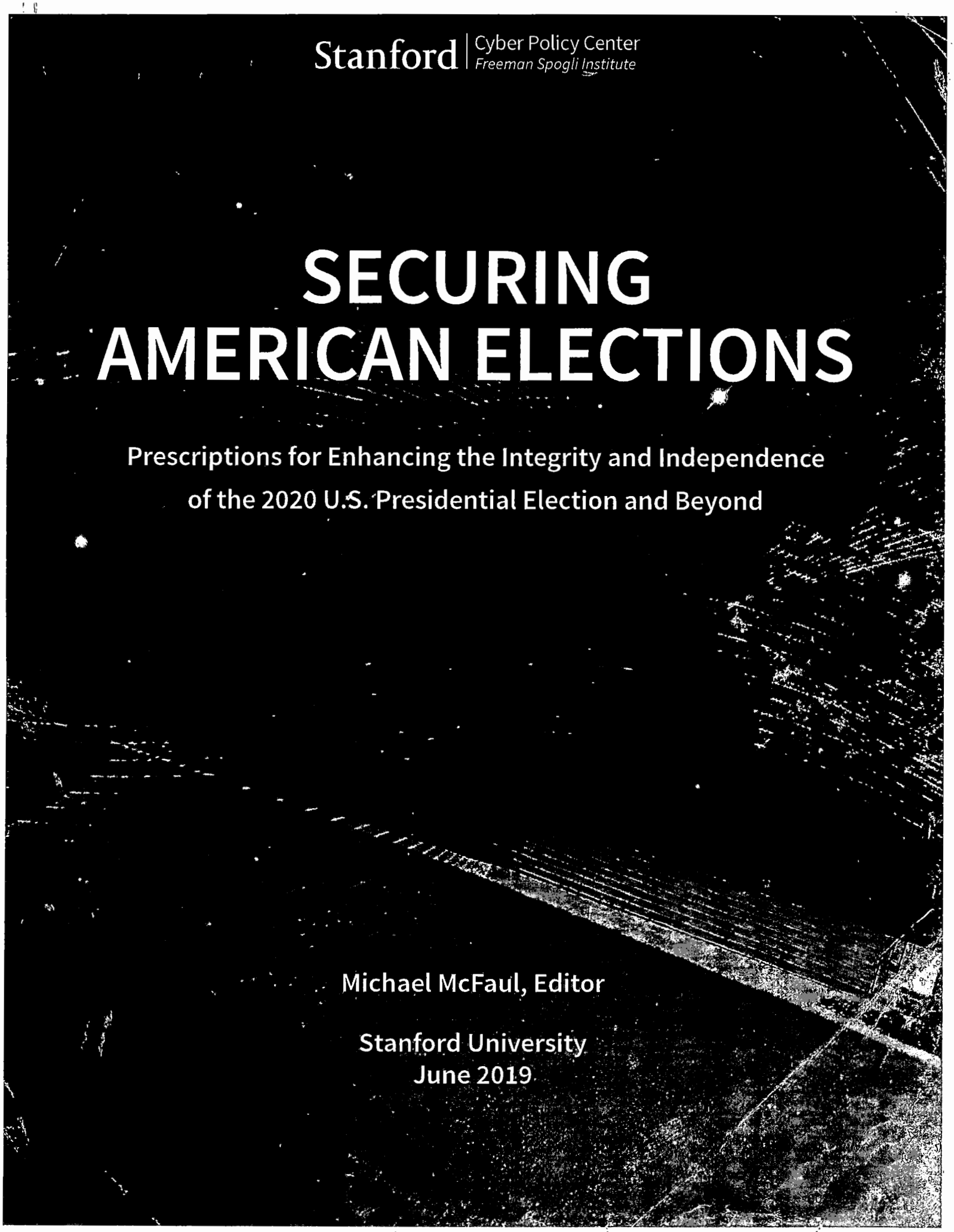

Stanford | Cyber Policy Center
Freeman Spogli Institute
SECURING AMERICAN ELECTIONS
Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond
Michael McFaul, Editor
Stanford University
June 2019

TABLE OF CONTENTS

PREFACE

By Michael McFaul

In 2016, Russia attacked the United States. As the Special Counsel report stated, "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[1] More precisely, Russian President Vladimir Putin, his government, and his proxies deployed multiple strategies and instruments—media, doxing, covert operations, direct contacts with Trump associates, and cyber-attacks on U.S. electoral infrastructure—to influence the outcome of the 2016 U.S. presidential election, and more generally, to disrupt the electoral process. Although the Kremlin had intervened previously in the electoral processes of other countries and dabbled in influencing earlier American elections, the scale, scope, and sophistication of this Russian intervention in this American election were unprecedented.

In reaction to discoveries about Russia's election interference in 2016, many recommended the creation of a bipartisan, independent commission, similar to the commission established after the September 11th terrorist attacks, to investigate what happened, how the United States responded, and what policies should be adopted moving forward to prevent or at least minimize new attempts by Russia or other countries to interfere in American elections.[2] Unfortunately, that idea never took root. In May 2017, Deputy Attorney General Rod Rosenstein of the U.S. Justice Department instead appointed Robert Mueller as Special Counsel overseeing an investigation into the allegations of Russian interference in the 2016 U.S. presidential election and related matters. Mueller and his team have revealed detailed accounts of aspects of the Russian campaign and produced 34 indictments of both Americans and Russians, but his mandate was never to investigate all dimensions of the Russian operations.[3] Nor did he interrogate the Obama administration's responses to the Russian interference or offer policy prescriptions. Numerous Congressional committees have undertaken the challenge of investigating potentially illicit Russian activity—which some are continuing currently[4]—but none have thus far comprehensively examined the entirety of the Russian attack, or the American governmental and non-governmental responses (or lack thereof) to this foreign intervention. Moreover, the Mueller report lacks comprehensive policy recommendations for how to prevent foreign interventions in future U.S. elections. As discussed throughout this report, the executive branch has implemented several reforms to reduce the threat of foreign meddling in elections. The

U.S. Congress also has proposed several new bills to help the effort, many of which we endorse in this study. But the response so far does not meet the threat, which as FBI Director Christopher Wray warned in April 2019, remains very real.[5]

Outside of government, several books, articles, task forces, and non-governmental organizations have delivered critical insights regarding the Russian attack and proposed innovative policy prescriptions.[6] We endorse and amplify many of these ideas in our report. Nevertheless, the United States still has nothing on the shelf comparable to the 9/11 Commission Report, which contained not only analysis of what happened and why, but also significant policy prescriptions.

This study seeks to provide a partial substitute for such a commission report. Building on the abovementioned research and investigations, our report begins by summarizing in Chapter One what the Kremlin did in 2016 and why. Chapters Two through Eight then offer concrete prescriptions for protecting the integrity and independence of U.S. elections, focusing in particular on strengthening resiliency before the 2020 presidential election. Our recommendations are practical, concrete, and achievable before 2020—but they demand action now.

Our team of authors includes experts on cybersecurity, deterrence, Russia, social media companies, and American electoral regulations, as well as diplomacy, democracy and ethics.[7] Our view is that all of these disciplines must be brought to bear in order to develop a sophisticated, comprehensive, and successful strategy for repelling not only potential threats from Russia, but also attacks from other foreign and domestic actors seeking to disrupt the integrity of the U.S. electoral process. American voters must choose their leaders alone, without help or interference from outsiders. In this report, we suggest a strategy for enhancing the permissive conditions for just that—free and fair elections not shaped or undermined by the actions of foreign actors motivated by different aims or malign intentions. Our analysis and advice are non-partisan, animated by the belief that all Americans share a common interest in protecting the integrity and independence of the U.S. electoral process.

This report urges policymakers, in both government and the private sector, to act immediately in order to protect the integrity and independence of U.S. elections, particularly in the run-up to the 2020 presidential election, and recommends the following actions in order to do so:[1]

Increase the Security of the U.S. Election Infrastructure

2.1. Require that all vote-counting systems provide a voter-verified paper audit trail.

2.2. Require risk-limited auditing for all elections.

2.3. Assess the security of computerized election-related systems in an adversarial manner.

2.4. Establish basic norms regarding digital behavior for campaign officials.

2.5. Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.

2.6. Retain the designation of election infrastructure as critical infrastructure.

2.7. Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Regulate Online Political Advertising by Foreign Governments and Nationals

3.1. Explicitly prohibit foreign governments and individuals from purchasing online advertisements targeting the American electorate and aimed at influencing U.S. elections.

3.2. Support the passage of the Honest Ads Act with several key amendments.

3.3. Strengthen self-regulation mechanisms for the major internet platforms.

Confront Efforts at Election Manipulation from Foreign Media Organizations

4.1. Require greater disclosure measures for FARA-registered foreign media organizations.

4.2. Mandate additional disclosure measures during pre-election periods.

4.3. Support existing disclosure measures of specific social media platforms.

Combat State-Sponsored Disinformation Campaigns from State-aligned Actors

5.1. Create standardized guidelines for labeling content affiliated with disinformation campaign producers.

5.2. Create norms for the media's handling of stolen information.

5.3. Limit the targeting capabilities for political advertising.

5.4. Expand transparency for paid and unpaid political content.

5.5. Improve the quality and scope of detection tools and reporting policies for social media platforms.

5.6. Build an industry-wide coalition to coordinate and encourage the spread of best practices.

5.7. Remove barriers to the sharing of information relating to disinformation, including changes to privacy and other laws as necessary.

5.8. Establish a Social Media ISAC/ISAO to improve communication between the U.S. government and social media companies about disinformation operations.

5.9. Increase overall transparency on social media platforms.

5.10. Carefully balance platform responsibility with individual freedoms.

5.11. Establish a norm among candidates to not use stolen data or manipulated content.

5.12. Emphasize digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.

Enhance Transparency about Foreign Involvement in U.S. Elections

6.1. Mandate transparency in the use of foreign consultants and foreign companies in U.S. political campaigns.

6.2. Increase transparency about foreign business interests.

6.3. Disclose contacts with foreign nationals and governments.

6.4. Strengthen the norm of one government at a time.

Establish International Norms and Agreements to Prevent Election Interference

7.1. Fortify U.S. and international commitment to human rights.

7.2. Strengthen international norms protecting election infrastructures.

7.3. Create norms to deter the use of disinformation and hacked materials.

7.4. Lead international advocacy against foreign interference through disinformation.

7.5. Distinguish legitimate cross-border assistance from illicit or unlawful interventions.

7.6. Hold congressional hearings about policies to support free and fair elections internationally.

7.7. Promote cooperation among democracies focused on election protection.

7.8. Appoint a senior U.S. government representative on election interference.

7.9. Develop guidelines about platform cooperation with foreign governments.

Deter Foreign Governments from Election Interference

8.1. Recalibrate risk tolerances for actions in cyberspace.

8.2. Signal a clear and credible commitment to respond to election interference.

8.3. Maintain a visible position of U.S. capabilities, intentions, and responses.

8.4. Enact country-specific and timely responses that impose real, effective costs.

8.5. Promote collective engagement with international partners.

8.6. Conduct a continuous strategic disruption campaign against adversaries that seek to interfere with U.S. elections.

8.7. Pursue common interests in cyberspace where possible.

CHAPTER ONE

Understanding Putin's Intentions and Actions in the 2016 U.S. Presidential Election

By Michael McFaul and Bronte Kass

According to Russian President Vladimir Putin, the United States is a hostile power and a serious threat to Russian national interests. From his KGB days, Putin developed an analytical framework with regards to international politics, which cast the United States as the central enemy of the Soviet Union. His ideas evolved over time. After September 11, 2001, for instance, Putin pivoted towards greater cooperation with President George W. Bush in a common fight against terrorism. During Dmitry Medvedev's presidency, then Prime Minister Putin also allowed greater cooperation between the United States and Russia. Today, however, Putin has returned to his earlier ideas. Putin's animosity towards the United States has increased during his third and fourth terms in office, animated by a belief that the United States aims to undermine his rule and weaken Russia more generally.

Putin now is engaged in an international ideological struggle that he defines as a contest between conservative, Christian, sovereign values—which he embraces—and decadent, liberal, multilateral ideas championed by many Western governments, including first and foremost the United States. When given the opportunity, Putin seeks to weaken the United States and advance his ideology of 'Putinism'. The 2016 presidential election in the United States offered Putin one of those opportunities.

'Putinism' as a Transnational Ideology and International Campaign

Regarding international affairs, Putin increasingly has championed the sovereignty of great powers like Russia and criticized what he considers American hegemony.[2] In Putin's view, the liberal international order established after World War II serves American national interests at the expense of other countries. Putin also contends that the United States uses overt military power to violate the sovereignty of other countries, a claim backed by empirical evidence, including most recently, Serbia (1999), Afghanistan (2001), Iraq (2003), and Libya (2011). As Putin lamented in his speech before the 2007 Munich Security Conference, "Unilateral and frequently illegitimate actions have not resolved any problems. Moreover, they have caused new human tragedies and created new centers of tension... plunging the world into an abyss of permanent conflicts... One state and, of course, first and foremost the United States, has overstepped its

national borders in every way. This is visible in the economic, political, cultural, and educational policies it imposes on other nations. Well, who likes this? Who is happy about this?"[3] Other times, American presidents, according to Putin, deploy covert means to destabilize or overthrow regimes, be it in Serbia (2000), the Arab Spring (2011), Russia (2011-2012), Ukraine (2013-2014), or Venezuela today.[4]

It is Russia's mission, therefore, to resist and prevent American attempts at regime change as well as to weaken American power more generally in the international system. To achieve these objectives, Putin has been strategically investing in resources that strengthen his capacity to counter the United States. For example, Putin has increased military spending to modernize the Russian army, produce improved weapons, and better train soldiers. These increases in military capabilities were on display in Georgia in 2008, Ukraine in 2014, and Syria in 2015. Russian nuclear modernization, both of warheads and delivery vehicles, also has expanded during Putin's presidency. Putin also has invested heavily in Russia's cyber capabilities. In 2007, Putin launched what many consider 'the first cyber war' against Estonia, and then accompanied Russia's physical intervention into Georgia in August 2008 with cyber-attacks. Ukraine has similarly endured numerous cyber assaults since Russia's intervention in 2014.

In addition to expanding military and cyber capabilities, Putin and the Kremlin also have fostered ideological alliances around the globe, including within liberal democracies and countries formally aligned with the United States. Over the years, Putin has won over many sympathizers throughout Europe, including Prime Minister Viktor Orbán in Hungary, Marine Le Pen in France, Brexit champion Nigel Farage in the United Kingdom, Geert Wilders in the Netherlands, President Andrzej Duda in Poland, Deputy Prime Minister Matteo Salvini in Italy, and Prime Minister Andrej Babiš in the Czech Republic. The rise of these populist leaders has fostered a perception of a successful, coordinated, populist, illiberal global movement with Putin as its spiritual anchor.

In parallel, Putin and his proxies have enhanced ties between Russian and foreign non-governmental organizations with a shared ideology. Russian Houses have sprouted all over the world to propagate Putinism, and the Russian Orthodox Church has developed connections with conservative religious groups around the world, including in the United States. Moreover, strengthened Russian relations with non-governmental organizations, such as the National Rifle Association (NRA), are an important component of this global strategy to nurture ties with like-minded European and Americans.[5] At times, Russian actors have even provided direct financial resources to fellow ideological travelers.[6]

To further propagate his ideas abroad, Putin has allocated significant resources to developing several media outlets and social media platforms. In the Russian-speaking world, particularly in countries that gained independence after the Soviet collapse, the Kremlin has devoted massive resources to maintaining an influential expanse of Kremlin-controlled television networks, radio, and other media. To extend beyond the Russian-speaking world, the Kremlin started the media company Russia Today in 2005, later renamed RT to disguise its affiliation. With an

annual budget of over $300 million USD, RT now broadcasts in 6 languages and has claimed to be YouTube's most-watched media company with nearly 3 billion views (of which 1.5 billion are from its flagship English-language channel).[7] In 2014, the Russian government also created Sputnik, an organization that serves as a news agency, news website, and radio broadcast service. The Kremlin-controlled platform promotes a pro-Russian slant on politics, economics, and public opinion, which its regional bureaus gear specifically toward a non-Russian audience.

In parallel with these efforts, Putin and his proxies have invested in the means to circulate disinformation and shape political discourse on social media platforms, including most famously through the Internet Research Agency (IRA). As detailed in the Special Counsel report, the IRA orchestrated a multi-pronged intervention specifically during the 2016 U.S. presidential election, but notably, the IRA and other Russian agents have been conducting disinformation operations on social media platforms for several years in many countries around the world.[8] Other Russian actors in the digital world use social media platforms to push pro-Putin, anti-American ideas.

The Russian army and ethnic Russian separatists constitute a final blunt instrument of propagating 'Putinism'. Putin's annexation of Crimea in 2014 and intervention in eastern Ukraine later that year occurred in parallel with a massive ideological campaign to persuade ethnic Russians in these regions to embrace Putin's worldview. Putin's recent proposal to provide Russian citizenship to ethnic Russians living in eastern Ukraine, just as he did to residents in the Georgian territories of Abkhazia and South Ossetia, is another key attempt to undermine the sovereignty of a neighbor in the pursuit of his expansionist, ideological agenda.[9]

Putin's Preferences in the 2016 U.S. Presidential Election

By 2016, Putin's anti-American, anti-liberal, and anti-democratic perspective had crystalized, while simultaneously, his instruments for exporting and propagating his worldview were increasing substantially. Ideological intent and enhanced capability combined to produce the most comprehensive Russian interference campaign thus far in an American election.

Putin initially aimed to delegitimize the American electoral process and American democracy more generally. For years, Putin had endured what he believed were lectures from Western critics about the autocratic elements of Russia's system of government. Putin was particularly annoyed with Secretary of State Hillary Clinton's criticism of the lack of freeness and fairness of the electoral process in the December 2011 parliamentary election in Russia, an "attack" which Putin said publicly sent a signal to the Russian opposition to protest against his government.[10] Consequently, Putin wanted to sow division, disrupt processes, and more generally cast doubt about the integrity of the 2016 U.S. presidential election.

Putin also aimed to weaken Clinton's presidential candidacy and help Trump as another means for undermining the integrity of the 2016 election. The unexpected emergence of Trump as a viable candidate offered Putin more opportunities to advance his agenda against American democracy. Supporting Trump became a central part of Putin's strategy of delegitimization. Although easy to forget now, Trump was not considered a serious candidate at the beginning

of the campaign, as he was regarded as a provocateur and disrupter outside of the mainstream. Eventually, he would even directly challenge the legitimacy of the American democratic process himself, berating subjects such as the unfair primary process, "fake news", and the corrupting influence of money in politics. As Election Day approached, Trump even warned that the vote was going to be rigged.[11] Supporting such an unpredictable and oftentimes inflammatory candidate therefore served Putin's goal of undermining the integrity of American democracy.

In addition, as a candidate, Trump expressed many policy positions that Putin openly endorsed. For instance, candidate Trump pledged to look into lifting sanctions and recognizing Crimea as part of Russia.[12] Trump campaign representatives tried to change the Republican Party platform to eliminate support for lethal weapons for Ukraine. Trump frequently criticized the NATO alliance, while barely saying a word about democracy and human rights.[13] When asked about Putin's human rights abuses inside Russia, Trump defended Putin with a narrative of 'whataboutism', arguing, "Well, I think our country does plenty of killing also…."[14] After winning the election, he later pushed back on criticism of Putin by stating, "We have a lot of killers…you think our country is so innocent?"[15] On the campaign trail, Trump predicted, "We're going to have a great relationship with Putin and Russia."[16] Trump has also praised Putin personally and profusely,[17] describing him as "brilliant"[18] and a "genius",[19] and suggesting that he was a better leader than Obama, when he asserted, "I will tell you in terms of leadership [Putin] is getting an 'A', and our president is not doing so well…"[20] It was very rational, therefore, for Putin to want Trump to win, even if the Trump administration did not follow through on many of these pro-Putin campaign statements.[21] As the unclassified report by the Office of the Director of National Intelligence on Russian involvement in the 2016 U.S. presidential election concluded, "We assess Putin, his advisers, and the Russian Government developed a clear preference for President-elect Trump over Secretary Clinton."[22] Putin himself then affirmed this assessment of the American intelligence community. When asked point blank about his electoral preferences during the press conference at the summit in Helsinki in July 2018, Putin answered bluntly, "Yes. I wanted him to win, because he talked about the normalization of U.S.-Russia relations."[23]

Conversely, Putin loathed Clinton. Putin did not want to see continuity in American foreign policy. Well before becoming a presidential candidate, Clinton had earned a reputation in Putin circles as a hawk. As a candidate, she said nothing to dispel that image. On Russia, she advocated the opposite of Trump: recognition of Crimea as Ukrainian territory, increased sanctions, a need to strengthen NATO, and a commitment to advocating for greater freedom inside Russia. Ideologically, Clinton espoused liberal internationalism, the exact opposite of Putin's worldview. Putin also seemed to harbor personal animosity towards Clinton, beyond just policy differences or her criticism of the procedures in the 2011 parliamentary elections. As Clinton wrote in her latest memoir, "Our relationship has been sour for a long time."[24]

The Multi-Pronged Russian Intervention

Putin not only had a personal preference in the 2016 U.S. presidential election, but also greenlighted multiple efforts to help his preferred candidate win. Confirming what U.S. intelligence had assessed two years earlier, the Special Counsel investigation headed by Robert Mueller established that the Kremlin perceived it would benefit from a Trump presidency and thus worked diligently to secure that outcome. According to the Special Counsel report, "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[25] The unredacted portion of the Special Counsel report focused on two influential Russian operations: (1) computer-intrusion operations against the Clinton campaign and Democratic Party officials and (2) a social media campaign that favored candidate Trump and disparaged candidate Clinton.[26] The U.S. Department of Justice later determined that Russia's principal interference operations violated U.S. criminal law. Many of the individuals and entities involved in the social media campaign "have been charged with participating in a conspiracy to defraud the United States by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections, as well as related counts of identity theft."[27] Russian intelligence officers who carried out the hacking also have been charged for violating federal laws.

The overall Russian campaign, however, was wider than these two operations, and included traditional media messaging, offers of compromising materials on one candidate in support of another, possible counterintelligence efforts by Russian agents to create leverage over several individuals in Trump's orbit, and preparations to disrupt voter registration logs and even vote counts on Election Day.[28]

Publishing Stolen Information

All countries with the capacity to do so—including Russia—gather human intelligence (HUMINT) and signals intelligence (SIGINT). Regarding HUMINT collection, the Kremlin ran an aggressive campaign to build personal relationships with Trump campaign officials in 2016. Clinton and her team were considered a known entity to Moscow, but they knew significantly less about Trump and therefore vigorously cultivated contacts to learn more about the candidate and his advisors. As a good diplomat should, Russia's Ambassador to the United States, Sergey Kislyak, boldly reached out to and successfully met several key Trump advisors, including future National Security Advisor Michael Flynn, future Attorney General Jeff Sessions, and future White House senior advisor Jared Kushner. Kislyak mingled with VIPs at candidate Trump's one major address devoted to foreign policy, and he attended the Republican National Convention, while skipping the Democratic National Convention. Other Russian actors with close Kremlin ties cultivated relationships with Trump campaign advisors George Papadopoulos, Paul Manafort, and Carter Page.

Collecting intelligence is one thing; stealing it illicitly and publishing it extensively is quite another. In April 2016, Russian intelligence officers—i.e., the Main Intelligence Directorate of the General Staff of the Russian Army (commonly known as GRU)—hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) and stole hundreds of thousands of documents, including significant amounts of data pertaining to internal strategy documents, fundraising data, personal identifying and financial information, opposition research, and employee emails.[29] Two GRU military units were discovered to have facilitated the computer intrusions: Military Units 26165 and 74455.[30] Military Unit 26165 is a GRU cyber unit dedicated to targeting military, political, governmental, and non-governmental organizations outside of Russia.[31] Starting in March 2016, Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as email accounts of individuals affiliated with the Clinton campaign.[32] Military Unit 74455 is a related unit with multiple departments engaged in cyber operations, whose officers assisted in the release of documents stolen by Unit 26165, the promotion of those releases, and the publication of anti-Clinton content on social media accounts.

GRU officers also sent hundreds of spear-phishing emails to the work and personal email accounts of Clinton campaign employees and volunteers.[33] Through a hacking operation, the GRU stole tens of thousands of emails from John Podesta, the chairman of Clinton's campaign. By April 2016, the GRU had gained access to the DCCC computer network using stolen credentials from a DCCC employee who had been successfully spear-phished. The GRU then traversed the network and continued to steal access credentials along the way, ultimately compromising approximately 29 computers. On April 18, 2016, the GRU gained access to the DNC network via a Virtual Private Network between the DCCC and DNC networks, compromising over 30 computers on the DNC network, including the mail server and shared file server.[34] Unit 26165 implanted two types of customized malware known as "X-Agent" and "X-Tunnel", a credential-harvesting tool, and a tool used to compile and compress materials for exfiltration onto the DCCC and DNC networks.[35]

Although unnerving, there is nothing unusual about either human or electronic data collection by the Russian government during the 2016 U.S. presidential election. The subsequent publication of this stolen data, however, was extraordinary and unprecedented. Russian agents carried out the anonymous release of this information through two fictitious online personas—DCLeaks and Guccifer 2.0—and later through third-party websites, including most importantly WikiLeaks. The GRU began posting stolen documents in June 2016.[36] While Russian cyber agents had compromised cybersecurity systems and stolen data from both the Republican and Democratic parties, the U.S. intelligence community discovered that they decided not to publish the data obtained from the Republican Party.

On June 14, 2016, the DNC and its cyber-response team announced the breach of the DNC network and suspected theft of DNC documents.[37] Guccifer 2.0 released thousands of stolen documents in a series of blog posts between June 15, 2016 and October 18, 2016.[38] According to

the Special Counsel report, "documents included opposition research performed by the DNC (including a memorandum analyzing potential criticisms of candidate Trump), internal policy documents (such as recommendations on how to address politically sensitive issues), analyses of specific congressional races, and fundraising documents. Releases were organized around thematic issues, such as specific states (e.g., Florida and Pennsylvania) that were perceived to be competitive in the 2016 U.S. presidential election."[39]

In order to expand their influence, the GRU units decided to transfer many of the documents to WikiLeaks. WikiLeaks founder Julian Assange had expressed opposition to candidate Clinton well before the first release of stolen documents.[40] His strong animosity stemmed in particular from then-Secretary of State Clinton's fierce condemnation of his role in facilitating "Cablegate"—WikiLeaks's controversial release of over 250,000 unredacted and previously classified U.S. diplomatic cables in 2010.[41]

In total, WikiLeaks released over 50,000 documents stolen from Podesta's personal email account.[42] On July 6, 2016, WikiLeaks contacted Guccifer 2.0 through Twitter's private messaging function, writing "if you have anything hillary related we want it in the next tweo [sic] days prefable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after." The Guccifer 2.0 persona responded, "ok ... i see." WikiLeaks also explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."[43] As reports attributing the hacks to the Russian government emerged, WikiLeaks and Assange made several public statements to obscure the source of the released materials and continued similarly cryptic behavior after the U.S. intelligence community publicly announced its assessment that Russia was behind the hacking operation.

Trump and his campaign officials showed interest in WikiLeaks's releases of hacked materials during the summer and fall of 2016.[44] According to his former deputy campaign chairman Richard Gates, Paul Manafort expressed excitement, wanting to be kept apprised of developments and future releases.[45] Donald Trump Jr. had direct communications with WikiLeaks during the campaign period.[46] On October 12, 2016, WikiLeaks wrote to Trump Jr. that it was "great to see you and your dad talking about our publications. Strongly suggest your dad tweets this link if he mentions us wlsearch.tk."[47] WikiLeaks wrote that the link would help Trump in "digging through" leaked emails and stated "we just released Podesta emails Part 4."[48] Two days later, Trump Jr. publicly tweeted the wlsearch.tk link.[49] Candidate Trump encouraged Russia and WikiLeaks to do more, declaring on July 27, 2016, "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press." According to the Special Counsel report, "Trump made this request repeatedly, and [Michael] Flynn subsequently contacted multiple people in an effort to obtain the emails."[50] Within approximately five hours of Trump's statement, Unit 26165 officers targeted Clinton's personal office for the first time.[51]

WikiLeaks timed the publication of these emails and documents to maximize their disruptive effect. The stolen emails, accompanied by conservative commentary, generated a narrative of

unfair treatment of presidential candidate Bernie Sanders by the DNC. Supporters of Sanders were outraged, booed Clinton during the Democratic National Convention's opening ceremony and even picked up Trump's "lock her up" slogan during their protests. This scandal generated by Russian activity forced then-DNC Chair Debbie Wasserman Schultz to resign before she could open the party's convention. Beyond the specific allegations of DNC bias against Sanders, the publication of these emails fueled the more general narrative of Clinton being corrupt and insincere.

Strategic timing of this "doxing" campaign helped the Trump campaign to navigate potential pitfalls. On October 7, 2016, The Washington Post published an Access Hollywood video that captured candidate Trump using graphic language about women that was expected to adversely affect his campaign. Less than an hour after the video's publication, WikiLeaks released the first set of emails stolen from Podesta's account.[52] Print and broadcast media devoted considerable attention to the content of these stolen data.

Rather than criticizing the electoral interference, Trump encouraged the WikiLeaks operation, declaring "I love WikiLeaks" while on the campaign trail and calling on this foreign organization to continue publishing his opponent's private communications. By one count, Trump mentioned WikiLeaks over 160 times in the last month of the campaign.

Before 2016, no foreign government had ever attempted to steal data from American politicians and then publish this information as a means to significantly influence the electoral outcome. This element of Putin's strategy to influence the 2016 U.S. presidential election was the most impactful.[53]

Russian Media Campaigns, Disinformation Social Media Operations, and Physical Rallies

In parallel to publishing stolen data, the Kremlin orchestrated a multi-pronged media campaign within the United States designed to help Trump, hurt Clinton, and foster division within American society more generally. This campaign—part disinformation and part partisan commentary—was comprised of several methods.

One instrument of swaying American voter attitude was the use of traditional media. Russian state-controlled media produced pro-Trump and anti-Clinton content targeted at American voters. The Russian state-controlled television network RT broadcasted within the United States, appearing in 85 million households though cable bundles and as one of the most watched television channels on YouTube. For YouTube, RT produced a variety of anti-Clinton clips, claiming for instance that the Clinton Foundation paid for Chelsea Clinton's wedding, that Clinton created the conditions for ISIS, that Clinton and ISIS are funded by the same money, and that 100% of Clinton charity proceeds went to themselves. Sputnik also produced anti-Clinton, pro-Trump content, and then circulated these messages on multiple platforms, including Facebook and Twitter. When tweeting out #CrookedHillary, Sputnik made the Kremlin's preferences clear.

Second, Russian-operated Twitter and Facebook accounts then amplified the anti-Clinton, pro-Trump messaging. A key player in these social media activities was the IRA. Based in St. Petersburg with funding from Russian oligarch Yevgeniy Prigozhin, a close colleague of Putin, the IRA evolved from a generalized program designed in 2014 to undermine the integrity of the U.S. electoral system, into a targeted operation that by early 2016 was supporting candidate Trump and criticizing candidate Clinton. Its operations also included the purchase of political advertisements on social media in the names of fictitious U.S. persons and entities, as well as the staging of political rallies inside the United States.[54] In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled accounts that collectively made 80,000 posts between January 2015 and August 2017, reaching at least 29 million U.S. persons, but potentially an estimated 126 million persons overall.[55] According to Facebook, the IRA purchased over 3,500 advertisements, and the expenditures totaled approximately $100,000.[56] In January 2018, Twitter announced the identification of 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million individuals who may have been in contact with an IRA-controlled account.[57] According to recently published materials, Russian bots also retweeted Trump more than 470,000 times during the final months of election.[58] In addition, Russian-linked accounts were responsible for 48-73% of the retweets of WikiLeaks' tweets during the same time period.

Dozens of IRA employees, known as 'specialists', were responsible for operating accounts and personas on different social media platforms. By early 2015, the IRA began to create larger social media groups or public pages that claimed to be affiliated with U.S. political and grassroots organizations. In certain cases, the IRA designed accounts to mimic real U.S. organizations, but it more often created fictitious accounts, posing as anti-immigration groups, Tea Party activists, Black Lives Matter protestors, and other social and political activists. In November 2017, lawmakers released a collection of Russian-sponsored ads—featuring themes such as the Benghazi attack, border security, gun safety, the Black Lives Matter movement, and Texas secession—that were specifically aimed at U.S. Facebook and Instagram users.[59] IRA employees have acknowledged that their work focused on influencing the results of the 2016 U.S. presidential election.[60]

Throughout 2016, IRA accounts published an increasing number of materials supporting Trump and opposing Clinton. As early as March 2016, the IRA purchased advertisements that overtly opposed the Clinton campaign. The first known IRA advertisement explicitly endorsing the Trump campaign was purchased on April 19, 2016 as an advertisement on the Instagram account "Tea Party News" asking for help to "make a patriotic team of young Trump supporters" by uploading photos with the hashtag "#KIDS4TRUMP."[61] Dozens of advertisements supporting the Trump campaign were subsequently purchased, predominantly through the Facebook groups "Being Patriotic", "Stop All Invaders", and "Secured Borders."

Collectively, the IRA's social media accounts reached tens of millions of Americans through either operating accounts to pose as individual persons, or controlling a network of automated

accounts to amplify existing content.[62] Moreover, the IRA used social media platforms to organize protests in the United States and successfully encouraged tens of thousands of Americans to RSVP for their political events. According to the Special Counsel report, the IRA would recruit a real U.S. individual to serve as an event coordinator, promoting the event by contacting American media, and sharing videos or photographs of the event afterwards. The earliest evidence of a facilitated event was a "confederate rally" in November 2015.[63] In another example a year later, between 5,000 and 10,000 protesters in Manhattan attended a November 2016 anti-Trump protest organized by a Russian-linked group, seeking to capitalize on exacerbating racial tension.

The IRA continued to organize rallies even after the 2016 U.S. presidential election, although attendance varied. In addition, IRA employees were instructed to target specific American individuals that could be used to further advance their operational goals through amplifying IRA-posted content on social media platforms, such as persons whom they had successfully tasked with organizing rallies or taking photos with certain political messages.[64]

As per Robert Mueller's indictment of 13 Russians and 3 companies involved in interfering with the 2016 U.S. presidential election, "Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by Defendants. Defendants also used the stolen identities of real U.S. persons to post on [IRA]-controlled social media accounts. Over time, these social media accounts became Defendants' means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016." The goal of the "troll factory", according to the indictment, was to sow discord in the U.S. political system, particularly during the 2016 U.S. presidential election.

Often referred to as the "translator project", the IRA's U.S. department is subdivided into different responsibilities, including operations on social media platforms, analytics, graphics, and IT.[65] The IRA's U.S. department is part of a larger set of interlocking operations known as 'Project Lakhta',[66] and employees were aware that Prigozhin was involved in the IRA's U.S. operations. In May 2016, IRA employees, claiming to be U.S. social activists and administrators of Facebook groups, boldly recruited Americans to hold signs (including one in front of the White House) that read "Happy 55th Birthday Dear Boss", as an homage to Prigozhin himself (whose 55th birthday was on June 1).[67]

Led by general director Mikhail Bystrov and executive director Mikhail Burchik, the IRA began hiding its funding and activities as early as the spring of 2014. The IRA's resources and budget were incredibly vast. According to Mueller's indictment, "The [IRA] employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The [IRA]'s annual budget totaled the equivalent of millions of U.S. dollars."[68] Russian journalists reported that by the summer of 2016, the IRA's U.S. department employed around 80-90 people, a mere one-tenth of the IRA's total workforce, and cost

approximately $1 million per year just in salaries alone. The monthly ad spend was approximately $5,000 for a total of $120,000 in two years. Thus, less than a hundred people were creating and posting approximately 1,000 pieces of content, which was seen by 20-30 million people every week. For example, in August 2016, 15 million people in the United States saw at least one IRA-created ad per week, and in October 2016 the number of weekly impressions had reached its height of 70 million people.

IRA employees even succeeded in traveling to the United States on intelligence-gathering missions. In June 2014, four IRA employees applied to the U.S. Department of State to enter the United States, while lying about the purpose of their trip and claiming to be four friends who had met at a party.[69] Ultimately, according to the Special Counsel report, two IRA employees named Anna Bogacheva and Aleksandra Krylova received visas and entered the United States on June 4, 2014.

Russian Offers of Business Opportunities and Kompromat

In addition to publishing stolen data and implementing an extensive media campaign to influence the outcome of the 2016 U.S. presidential election, the Russian government and its surrogates reached out directly to the Trump campaign through "business connections, offers of assistance to the Campaign, invitations for Campaign officials and representatives of the Russian government to meet, and policy positions seeking improved U.S.-Russian relations."[70]

Kremlin-connected individuals and media entities began showing interest in Trump's campaign shortly after he announced his candidacy in June 2015.[71] According to the Special Counsel report, early contact was made in connection with a Trump Organization real-estate project in Russia known as 'Trump Tower Moscow', for which candidate Trump signed a Letter of Intent by November 2015. In January 2016, Trump Organization executive Michael Cohen had emailed and spoken about the project with the office of Kremlin Press Secretary Dmitry Peskov. While negotiations were led by Cohen, Trump associate Felix Sater provided assistance and daringly suggested the project would increase candidate Trump's chance of being elected.[72] Ultimately, the Trump Organization pursued the project through at least June 2016, including the consideration of travel to Russia by Cohen and candidate Trump himself.[73]

In parallel with the Trump Tower Moscow project, the Trump Organization maintained numerous business contacts with Russian individuals and entities. These connections spanned a multitude of actors from the Kremlin and other associates of Putin, who had a natural interest in strengthening their relationships with Trump campaign team members—despite their varying degrees of closeness to Trump himself. In the unclassified sections of the Special Counsel investigation, however, none of these business interests were deemed to be illegal.

In late April 2016, campaign foreign policy advisor George Papadopoulos was told by London-based professor Joseph Mifsud, immediately after Mifsud's return from a trip to Moscow, that the Russian government had 'dirt' on Hillary Clinton in the form of thousands of emails. One week later, in May 2016, Papadopoulos suggested that the Trump campaign had received

indications from the Kremlin that it could assist the campaign through the anonymous release of information damaging to Clinton.[74] For several months thereafter, Papadopoulos worked with Mifsud and two Russian nationals to arrange a meeting between campaign officials and the Kremlin, which ultimately never took place.

Russian outreach continued into the summer of 2016. On June 9, 2016, Donald Trump Jr., campaign chairman Paul Manafort, and senior campaign advisor Jared Kushner met in Trump Tower with a visiting Russian delegation headed by Russian lawyer Natalia Veselnitskaya. Before traveling to New York, Veselnitskaya coordinated her talking points with Russian Prosecutor General Yuri Chaika, one of the most senior officials in the Russian government and a close associate of President Putin. According to the Special Counsel report, "The written communications setting up the meeting showed that the Campaign anticipated receiving information from Russia that could assist candidate Trump's electoral prospects."[75]

Robert Goldstone had arranged the meeting. During the 2013 Miss Universe pageant in Moscow, Goldstone first met Trump and later became an acquaintance after working as a publicist for Russian performer Emil Agalarov, the son of Aras Agalarov, who was Trump's partner in hosting the pageant. In an email from June 3rd titled, "Russia – Clinton – private and confidential", Goldstone informed Trump Jr. that Veselnitskaya was bringing compromising information on Clinton and her campaign, as part of the Kremlin's effort to assist Trump's campaign. In response, Trump Jr. wrote back within minutes, "If it's what you say, I love it."[76]

At the meeting, Veselnitskaya made claims that funds derived from illegal activities in Russia were provided to Hillary Clinton and other Democrats, although she was unable to provide evidence when pressed. (Bizarrely, Putin affirmed this same conspiracy during his press conference with President Trump at their Helsinki summit in July 2018 when Putin accused British businessman Bill Browder of laundering money out of Russia and then providing a portion of these funds to the Clinton campaign.)[77] She then turned to criticizing the Magnitsky Act, a 2012 statute that imposed financial and travel sanctions on Russian officials, which had triggered a retaliatory ban on the adoption of Russian children.[78] Although she seemingly provided nothing concrete in this meeting, Veselnitskaya appeared to be trading kompromat on Clinton in return for sanctions relief. Veselnitskaya made several targeted efforts to follow up on the meeting, but the Trump team did not engage.[79] However, one day after this meeting, Trump teased that he planned to give a major speech that would reveal very damaging information about Hillary Clinton and the Clinton Foundation. He never delivered such a speech.

Russian officials continued to hold numerous meetings with senior Trump advisors. By one count, during the campaign and transition period, Russians met with 12 Trump campaign officials and associates during the course of 19 in-person meetings and over 50 communications. Most mysteriously, in August 2016, Manafort met his long-time business associate Konstantin Kilimnik, who had requested the meeting in order to deliver a peace plan for Ukraine that Manafort later acknowledged as a 'backdoor' way for Russia to control part of eastern Ukraine.[80] They also discussed the status of the Trump campaign and Manafort's strategy for winning

Democratic votes in Midwestern states. Months before the August meeting, Manafort had instructed his campaign deputy Gates[81] to provide Kilimnik with internal polling data, which Manafort expected to be shared with others in Ukraine and with Russian oligarch Oleg Deripaska.[82] Furthermore, Manafort met Kilimnik twice in the United States during the campaign period and conveyed campaign information, such as the strategic discussion of "battleground" states, which Manafort identified as Michigan, Wisconsin, Pennsylvania, and Minnesota.[83]

The Special Counsel investigation evaluated a series of additional links between Russian actors and the Trump campaign: outreach to two of Trump's then-recently named foreign policy advisors, dealings with a D.C.-based think tank that specializes in Russia and has connections with the Kremlin, events at the Republican National Convention, post-Convention contacts between Trump campaign officials and Kislyak, and other contacts through Manafort, who had previously worked for a Russian oligarch and a pro-Russian political party in Ukraine. Notably, the Special Counsel investigation established that "several individuals affiliated with the Trump Campaign lied to the Office and the U.S. Congress about their interactions with Russian-affiliated individuals and related matters... materially impair[ing] the investigation of Russian election interference."[84] The reasons for all of these meetings remains a mystery.

These meetings, usually initiated by Russian officials, produced subsequent suspicion about the intentions of Trump campaign officials and family members. While Putin explicitly wanted Trump to win, a Trump team delegitimized by multiple contacts with Russian officials—contacts that the Kremlin and Russian intelligence agents of course knew that American intelligence agencies would be monitoring closely—also served Putin's interests. The counterintelligence portion of the Special Counsel investigation has not been published and is most likely still ongoing.

Hacking of U.S. Electoral Infrastructure

Most disturbingly, Russian intelligence agents probed the U.S. electoral infrastructure in 2016. In June 2017, Samuel Liles, the Acting Director of the Department of Homeland Security's Office of Intelligence and Analysis Cyber Division, testified to the Senate Intelligence Committee that "Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors."[85] Beyond probing, the Special Counsel report specifically identified Russia's successful penetration of computers of one county government in Florida as well as successful placement of malware within VR Systems, a company that supplies Florida counties with voter registration systems.[86] VR Systems was also the provider of electronic poll books that malfunctioned in Durham Country, North Carolina in 2016.[87] Thankfully, Director Liles noted that there was no evidence that any hacking attempts in 2016 affected actual operations or outcomes, but implanted malware could still remain on these network systems and computers.

In addition, the Special Counsel report revealed that GRU officers also targeted election administrators and officials, including "U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities... [and] private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations."[88] By the summer of 2016, GRU officers were seeking access to state and local computer networks by exploiting known software vulnerabilities on the websites of state and local governmental entities. Through techniques such as "SQL injection", malicious code was sent to the state or local website in order to run commands, e.g., exfiltrating the database contents.

According to the Special Counsel report, "In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified."[89] Russian intelligence agents also sent spear-phishing emails to public officials involved in election administration and personnel at companies involved with voting technology.[90]

Despite having the capacity to do so, Putin and his agents decided not to try to disrupt these machines on Election Day itself. President Obama personally warned Putin about the consequences of Russian disruption of Election Day activities; perhaps this deterrence worked. Nonetheless, the mere fact that Russian cyber actors successfully penetrated and accessed the U.S. election infrastructure is highly concerning for its potential to undermine confidence in electoral outcomes in the future.

Measuring the Impact of the Russian Intervention

Russian activities played only a marginal role in influencing the outcome of the 2016 U.S. presidential election. Multiple other structural, institutional, and campaign factors were clearly more dominant in deciding the presidential election.[91] Furthermore, additional proximate events, such as pronouncements and non-pronouncements about ongoing FBI investigations, were influential on the final vote count. Without question, tens of millions of American voters cast their ballots for Trump or Clinton with no influence whatsoever from Russian actions. In the vast sea of variables determining voter preferences, precisely measuring the independent causal influence of Russia's efforts during the 2016 U.S. presidential election is impossible.[92] Several Russian actions, after all, amplified the campaign activities of the Trump team and his surrogates, making the task of isolating a Russian causal role even harder. But small effects in the tightly contested election could have made a difference, despite being impossible to prove. Even if Russian interference played only a marginal role, this election was won in the margins–78,000 votes in only three states: Michigan, Pennsylvania, and Wisconsin.

Some correlations seem probative. Putin made his biggest impact on the 2016 campaign by

stealing and then publishing DNC and Podesta emails, an operation that sparked a major rift between Sanders and Clinton supporters. In post-election surveys, twelve percent of Sanders's supporters in the Democratic primaries reported that they voted for Trump in the general election.[93] Many Sanders supporters also decided to instead stay home. Approval ratings of Clinton as a qualified candidate decreased significantly in October 2016 after the WikiLeaks publication of Podesta emails.[94]

Moreover, Russian disinformation operations sought to suppress voter turnout.[95] In some swing states, especially among the African-American population, turnout among Democratic voters was significantly lower in 2016 (59.6%) than 2012 (66.2%). Targeted efforts by the Kremlin sought to explicitly and implicitly discourage African-Americans voters from going to the polls, as other Russian-backed efforts bolstered white extremism online.[96]

Russian efforts also actively promoted third-party candidates.[97] Votes cast for third-party candidates were significantly higher in 2016 than in 2012, including in several swing states.[98] Green Party candidate Jill Stein won 31,072 votes in Wisconsin (four times as many votes as she garnered in 2012), ten thousand more votes than Clinton lost to Trump by (22,748) in that state. Similarly, in Michigan, Stein won 51,463 votes; Clinton lost to Trump by 10,704. In Pennsylvania, Stein won 49,463 votes; Clinton trailed Trump there by 44,292.

Again, it is impossible to say for certain that Russian actions played a decisive role in any of these outcomes. But to suggest that Russian intervention played no role seems implausible. That the Kremlin tried to influence the outcome of the 2016 U.S. presidential election is without question—and that the Kremlin should influence even the outcome of one voter in 2020 should not be permitted to happen.

Future Foreign Threats

Future online election interference will likely take three tracks: (1) the spread of disinformation intended to discredit political candidates and the political process, discourage and confuse voters from participating in elections, and influence the online discussion of political topics; (2) the use of information operations to disrupt election infrastructure during the electoral cycle, on the day of the election, and immediately afterward during vote tallying and result certification—including, but not limited to, changing vote records and tallies, interfering with the operation of voting machines, impeding communications between precincts and election operations centers, and providing disinformation that misdirects voters to the wrong polling place or suggests long wait times, incorrect ID requirements, or precinct closures that do not actually exist; and (3) the undermining of public confidence in electoral processes after the election takes place.[99]

Additional actors also should be expected to join Russia in future attempts to influence political discourse online, as the barriers to mounting disinformation campaigns will depend less on available computing power and technical skill, and more on the ability to quickly iterate among strategies, produce text in naturalistic English or another targeted native language, and identify psychological vulnerabilities in a target segment of the electorate.

Furthermore, new technologies, including deepfakes, AI text-generation engines, and more sophisticated networks of bots on Twitter and other sites that permit pseudonymous accounts, will continue to be used to spread disinformation, discredit candidates, confuse voters, and influence the discussion of divisive political topics. Notably, these technologies need not be fully convincing, nor capable of deceiving digital forensic auditors. A faked image or video that is convincing at first glance but later revealed to be a forgery will cast suspicion on other low-resolution or thinly-sourced images and video, and will ultimately serve to imbue the political process with doubt and resignation over the truth of any piece of political media. The spread of a viral hoax also can serve to push users off associated platforms, as seen in recent pushback against YouTube content aimed at children, which thereby narrows the channels through which information, including politically motivated information, is received and disseminated.

In testifying before Congress on his agency's preparations for the 2020 presidential elections, FBI Director Christopher Wray stated bluntly, "Make no mistake: The threat just keeps escalating and we're going to have to up our game to stay ahead of it..."[100] Wray is right, but it will take more than just the FBI upping their game to enhance the security and integrity of our next presidential election. Many other government agencies, the U.S. Congress, state governments, media and social media companies, the candidates and their campaigns, and all American voters more generally must also be involved. The remainder of this report offers concrete suggestions for how to do so.

CHAPTER TWO

Increasing the Security of the U.S. Election Infrastructure

By Herbert Lin, Alex Stamos, Nate Persily, and Andrew Grotto

The Problem

The existing technical infrastructure for facilitating U.S. elections includes computer-based electronic systems for both voter registration and vote casting. Although these systems are the primary focus of this chapter, other important parts of the entire electoral ecosystem include electronic poll books, vote tabulation systems, election night reporting systems on which news services rely, and auditing systems. This ecosystem is vast, decentralized in many places, and varies tremendously in its resilience to attack, therefore requiring substantial upgrades to advance its overall security.

In accordance with the Help America Vote Act (HAVA) of 2002, systems for voter registration are centralized at the state level.[1] The administration of voter registration databases entails a number of large-scale tasks, including (1) maintaining the correct status of individuals who are properly registered to vote and their relevant information on voter registration lists, (2) removing individuals who are no longer eligible to vote (e.g., those who have moved out of the jurisdiction) off registration lists, and (3) delivering precinct-by-precinct registration lists to the individual precincts where in-person voting occurs (e.g., creating and delivering paper-based or electronic poll books). By contrast, vote casting systems are decentralized down to the county level. Each county within the same state can use a different electronic voting system, which must include the following: (1) electronic voting systems that record ballots cast by citizens in person at individual precincts, (2) tabulation systems that record absentee ballots via postal mail, and (3) programs that tabulate vote totals at levels higher than the precinct.

Given the complexities of both systems, opportunities for internal error and hostile outside intervention abound. Small errors or deliberate disruptions can easily erode voter confidence in the electoral system. Vote casting systems and voter registration systems are components of a larger election ecosystem that includes political parties and candidate campaigns, traditional and non-traditional news media, poll workers, pollsters, and engaged citizens. Partisan stakeholders, who by definition want their candidates to win, add further complexity since they might be tempted to promote systems for voter registration and vote casting that favor their particular party or candidates and also are less secure than others available.

During the 2016 U.S. presidential election, a number of elements of the U.S. electoral infrastructure came under attack. The Special Counsel report described in detail these attacks carried out by the Main Intelligence Directorate of the General Staff of the Russian Army (GRU) on behalf of the Russian government.

> [I]n addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities... The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations.[2]

Moreover, the Special Counsel report specifically highlights:

> GRU officers... targeted state and local databases of registered voters using a technique known as 'SQL injection,' by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents) ... In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.

GRU officers also "sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology." As the Special Counsel report detailed, "In August 2016, GRU officers targeted employees of... a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network." Furthermore, "In November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. Election. The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer... The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government."[3]

Thankfully, there is no evidence that any votes were actually changed and that no lasting damage was done to voter registration databases. Nonetheless, these incidents should be viewed as precursors or dress rehearsals for similar attacks against the 2020 U.S. presidential election. As FBI Director Christopher Wray remarked in comparing the 2018 midterm elections to

the 2020 presidential race, "We recognize that our adversaries are going to keep adapting and upping their game... So we are very much viewing 2018 as just kind of a dress rehearsal for the big show in 2020...."[4]

Guaranteeing the integrity of the vote count is instrumental to a healthy democracy. Candidates and their campaigns have strong incentives to sway or portray the electoral processes in partisan terms, and thus those running elections, particularly election administrators, must do everything in their power to maximize the public's trust in their work. In a 2005 report still relevant today, the National Research Council asserted:

> [T]rusted election processes should be regarded as the gold standard of election administration, where a trusted election process is one that works, that can be shown to have worked after the election has been held, that can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and that can be shown to reflect the intent of the voters. Trusted election processes increase the likelihood that elections will be regarded as fair, even by the losing side and even in a partisan political environment.[5]

Because the majority of technology infrastructure supporting elections is computer-based, robust cybersecurity of the infrastructure is an essential element for assuring American voters that an election was conducted fairly. Providing such assurance is nevertheless complicated by three key challenges. First, all voters have a right to cast their ballots in secret, which cannot be compromised by election audits. Imagine, for example, the difficulty of developing a financial audit procedure for a bank in which particular monetary transactions of customers could not be associated with specific customers.

Second, an election must always produce a winner, even when only a few votes separate the results. A small number of fraudulent, improperly cast, miscounted, manufactured, lost, or otherwise invalid ballots can thus sway an election. Because small manipulations are simultaneously easier to perpetrate and inherently harder to detect than large ones are, the risk of election fraud is greatest when the electorate is evenly divided and vote counts are close, as has been the case recently for a number of American presidential elections.[6]

Third, the value of cybersecurity measures in many other computer-based systems can often be justified in cost-benefit terms, e.g., by comparing the cost of a particular security measure to the expected loss if the measure is not taken. In an election in a democracy, however, how does one measure the supposed value of a single vote? (Autocracies don't have to worry about such issues.) Budgets for cybersecurity are finite, thereby placing constraints on election administrators who must subsequently undertake careful assessment and evaluation of the security issues of the electoral infrastructure—both as a whole and for individual components.

Cybersecurity Considerations for the Overall Electoral Infrastructure

An unfortunate reality of information technology (IT) is that system testing can identify defects, including security vulnerabilities or software bugs, but no reasonable amount of system testing can prove that an IT-based system is completely free of defects. When a system is deployed for actual use, security becomes further complicated. The process of system certification can only evaluate the software and hardware that the vendor presents but cannot take into account how the system is actually operated and maintained when in use. It is even difficult to prove that the software running on a given machine in the infrastructure is the same as that which was presented for certification.

In addition, all software, including software for electoral infrastructure systems, contains bugs and other vulnerabilities that will be discovered after initial deployment, implying that a system that repairs any vulnerabilities known today may well be discovered to have vulnerabilities tomorrow. The assurance of security is therefore an ongoing process that requires searching for vulnerabilities proactively and fixing them immediately. This attribute of all software undergirds two necessary elements of electoral cybersecurity.

First, the assurance of security by checklist compliance—a requirement of the certification process—provides a baseline level of security, but by itself is known to be inferior to security assessed through an adversarial process. The best such process is an independent white-hat attack,[7] or a test attack conducted by white-hat teams that attempt everything real attackers would try by taking advantage of technological or procedural flaws in the system's security posture or the human infrastructure in which the technology is embedded. Security flaws uncovered by white-hat attacks are then forwarded to responsible parties for repairing.

Another type of adversarial process is an independent examination of the physical hardware and software of the system in question. Such examination will yield information about the system's ability to resist attack. Inspections before systems are deployed provide an opportunity for discovering the potential for bad behavior. However, vendors, who provide the hardware and software for elections, generally resist third party inspection of source code on the grounds that allowing outsiders such access compromises their intellectual property.

Second, "security by obscurity" is a poor security practice of relying predominantly on the secrecy of the system's design or implementation as the main method for ensuring its security.[8] By contrast, the responsible disclosure of discovered vulnerabilities is usually recommended, in order to provide strong incentives for system owners to address and fix them. (Under the practice of responsible disclosure, the system owner or vendor is notified of a vulnerability when it is discovered to ensure a quick resolution, and the vulnerability is publicly disclosed after a period of time that is deemed sufficient for repairing it.)

A few misconceptions about election cybersecurity also need to be briefly addressed. Many people commonly believe that the security of a computer can be assured by not connecting the computer to the internet. Although many attacks on computer systems are delivered through the internet, the lack of an internet connection does not guarantee security. For

example, an individual's computer could be compromised prior to ownership or while being updated, e.g., through using outdated operating systems with existing vulnerabilities, installing new programs or operating systems with additional files (e.g., backdoors or trojans that share information with a hacker), disabling an anti-virus or anti-malware program, or even monitoring power consumption.

Moreover, election officials themselves may compromise the election infrastructure, either wittingly or unwittingly, as cybersecurity is not solely a technical issue. Because human beings are intimately involved in all electoral operations, human vulnerabilities can certainly be exploited. Looking at the resilience of the electoral infrastructure as only or even primarily a technical issue is therefore a profound mistake, as many of the most harmful attacks on computer systems originate with an attacker targeting a human being.

Cybersecurity Considerations for Vote Casting Systems

For the acquisition of vote casting systems, election officials often rely on a process established by the Election Assistance Commission (EAC) certifying that a vendor's voting system meets the Commission's Voluntary Voting Systems Guidelines (VVSG), the latest of which were issued in 2015.[9] This certification is provided by any one of a number of voting system testing laboratories, which are accredited by the EAC and receive fees from vendors for their work in qualifying a system.

Because these standards include criteria related to security, election officials often view certification as complete assurance that a system's security is sufficient. Although the certification does confirm that the vendor paid attention to required security protocols, certification does not necessarily denote an adequate security posture. Moreover, even in states where verifiable systems are used, oftentimes a check on a voting system's functionality and accuracy does not take place.

A number of independent research efforts have demonstrated the ease with which individual electronic voting stations can be compromised by simply using the paltry resources available to university research teams.[10] Hostile foreign governments would be able to deploy orders of magnitude more resources to this task. In addition, these actors would have no qualms about attacking vulnerabilities or weaknesses that would yield higher leverage—in other words, engaging in vendor-level attacks such as installing damaging software or infiltrating outdated operating systems, as opposed to targeting specific machines to modify individual votes.

Verifying the security afforded by a given system's certification level is the first step in assuring overall election security. A second measure is to ensure that the properly certified system is the actual system deployed for use by voters, and not one that has been tampered with after its certification. Tampering opportunities occur at two stages: when the vendor loads software onto voting machines before they are shipped to precincts, and while voting machines sit in storage after delivery but before deployment and use.

Finally, a secure process must be established to address additional security risks when communicating the results from individual polling stations to a central tabulation authority. The received ballot totals must match those recorded at the precinct level. Such communication can be performed manually, by electronic transmission (e.g., over the internet or a phone line), or by physically carrying computer-readable media containing precinct-level vote totals to the tabulation authority's physical location. The security risks of each method can be mitigated with proper attention and even using more than one in parallel.

Types of vote casting systems currently vary from state to state.[11] Several states only allow vote by mail (e.g., Washington, Oregon, and Colorado), or paper ballot only (e.g., Michigan, Massachusetts, New York, and Virginia, among others). However, many have previously employed Direct Recording Electronic (DRE) voting machines without using a Voter Verified Paper Audit Trail (VVPAT) (e.g., Louisiana, Georgia, and South Carolina), or had mixed paper ballots and DREs without using VVPAT (e.g., Texas, Florida, Pennsylvania, Indiana, and Kentucky.) In total, fourteen states did not use VVPAT as their polling place equipment as of November 2018. This practice is dangerous.

Following the spark of public anger over Russian interference, states seeking to upgrade their vote casting systems have been caught between funding shortages, litigation challenges within procurement processes, or political deadlock. Despite these barriers, it appears that only Louisiana, South Carolina, and the majority of New Jersey, along with dozens of counties, will be using paperless voting machines in the 2020 U.S. presidential election.[12]

Nevertheless, it is still unclear whether the upgrades that have taken place thus far truly solve vote casting problems or simply create further security considerations, disguised by trust in new systems that lack thorough evaluation. For example, with the introduction of ballot-marking devices (BMDs),[13] a voter can use a touchscreen to vote, review a printed version of the ballot for verification and insert it into an optical scanner that counts and saves it in a secure lockbox. This paper trail consequently allows election officials to audit the election. Two primary concerns about the rollout of BMDs have been raised, however.[14] First, the system's printer and scanner share the same path, so if any races are left blank by voters, the machine could autofill the races—and neither election administrators nor voters themselves would be able to verify the change. Second, voters can opt to not review their ballot and send the vote directly to the scanner, thereby circumventing the exact process designed to confirm accuracy between the voter's intention and the actual counted ballot. It is also inevitable that future issues with BMDs would be dismissed or considered user error, leaving manipulation largely undetected. The New York State Board of Elections is reviewing certification due to these issues, but other jurisdictions, which have chosen to implement BMDs, are not.

In addition to the use of aging or unreliable vote casting machines, it should be noted that shortages of both physical equipment and human resources are likely, as resources for updating vote casting systems continue to be inadequate for effectively addressing future challenges.

Strengthened support must be provided to states and counties across the country that continue to conduct elections through vulnerable vote casting machines with insufficient ballot verification.

Cybersecurity Considerations for Voter Registration Systems

Voter registration systems differ from vote casting systems in a number of ways that affect their security posture. Most importantly, voter registration systems are centralized at the state level, giving the attacker the ability to have a bigger impact on manipulating or disrupting an election by compromising just a few voter registration systems, rather than the many voting machines that are not connected to a centralized system. Moreover, some voter registration systems rely on information from other databases, such as departments of motor vehicles, departments of correction, or departments of vital statistics, to confirm voter eligibility. Compromises in these databases, such as the alteration or erasure of key data, in turn could produce ripple effects on the accuracy of voter registration databases. Security issues with other databases could adversely affect the overall integrity of voter registration databases.

Voter registration systems also entail relatively straightforward computerized functionality that is present in many commercial database systems. Because the underlying software of voter registration systems is typically proven through applications to multiple problem domains and exercised repeatedly, they are less likely to be successfully hacked, but potentially more destructive in causing harm if ultimately compromised. By contrast, vote casting systems are niche products, put into operational use only sporadically, rendering them more vulnerable to concealed or undetected attacks that take place.

Finally, apart from requirements imposed by HAVA, voter registration databases are not required to conform to any set of national standards or guidelines for cybersecurity, thereby leaving the development and testing of such systems to each state. Although HAVA was the first U.S. law under which the federal government developed policies and provided funding for state and local elections, it lacks sufficient provisions with respect to uniform collection, reporting, and transparency of election-related data.[15] Nor does it mandate standards for voting technology and vote casting protocols.

Recommendations

In 2018, the National Academies released a consensus report entitled *Securing the Vote: Protecting American Democracy.*[16] This report made a number of recommendations intended to harden the election infrastructure of the United States against external attack and to safeguard its integrity and credibility. The authors incorporate all of these recommendations by reference, underscore the importance of several of them by mentioning them below, and go further by making a number of additional recommendations.

2.1. Require that all vote-counting systems provide a voter-verified paper audit trail.

New federal legislation should require that all vote casting systems must have the capability to provide a VVPAT for federal elections (NRC recommendation 4.11). Current guidelines for vote casting systems do not impose such a requirement, although existing regulations do provide specifications to which a VVPAT must conform if such a capability is used.

2.2. Require risk-limited auditing for all elections.

Legislation should require risk-limited auditing (NRC recommendation 5.8).[17] Through requiring voter-verified paper ballots, manual counting, and risk-limiting audits, the Protecting American Votes and Elections (PAVE) Act, introduced by Senators Ronald Wyden, Kirsten Gillibrand, Elizabeth Warren, Patricia Murray, Edward Markey, and Jeffrey Merkley, marks a positive step in this direction.[18] It would not only strengthen structures for risk-limiting audits and "provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved", but also improve access to voting systems for individuals with disabilities and make funding available to enhance the analysis and testing of accessible paper ballot verification mechanisms for "the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office."[19] It is recommended that similar legislation be introduced and enacted in a timely matter.

2.3. Assess the security of computerized election-related systems in an adversarial manner.

The security of computerized election-related systems should be addressed through a combination of white-hat attacks and independent code inspection. Without third-party examination or review of the systems' security, a key aspect of protecting U.S. election infrastructure will be neither publicized nor subject to independent scrutiny.

Legitimate concerns about intellectual property protection can be addressed through the use of carefully crafted non-disclosure and/or non-compete agreements. The former would permit public discussion of security flaws found but also specify details that could not be disclosed. Non-compete agreements would provide vendors with assurances that allowing code inspection would not enable those viewing code to become competitors. Findings from reports derived from white-hat attacks and code inspection could therefore be widely publicized to pressure vendors and election administrators to fix the problems without delay. Bug bounties, which incentivize individuals to report vulnerabilities through receiving recognition and compensation, should also be offered to encourage regular testing.

2.4. Establish basic norms regarding digital behavior for campaign officials.

In order to ensure the widespread adoption of improved cybersecurity practices during electoral cycles in particular, campaign officials should establish and uphold basic norms with regards to their own digital behavior.[20] For example, multi-factor or dual authentication is an easy practice to implement for confirming a user's claimed identity and strengthening

information security overall. In addition, improved processes for threat-intelligence sharing and disclosure of vulnerabilities would contribute to the development of digital behavior norms. Such efforts would illustrate that campaign officials not only take cybersecurity issues seriously, but are also raising overall levels of awareness and related action in the United States.

2.5. Commit regular funding streams to strengthen the cybersecurity posture of the election infrastructure.

Certain measures related to the organizations surrounding election infrastructure would enhance resilience and increase public confidence in the conduct of an election, and all of these measures will require increased funding. These include:

- The implementation of specific training programs for election administrators and their staff on basic cybersecurity practices (NRC Recommendation 5.2).[21]
- Extension of the voting period so that voters are able to cast their ballots over a period of time (e.g., several days). Entirely apart from making the voting process more convenient, it is simply a reality that technical problems often appear in complex computer-based equipment when placed into widespread operation with real users, and attempting to deploy fixes on a time scale of a few hours is often infeasible. An extended voting period would provide an opportunity to fix problems that appeared early, and voters unable to cast votes because of such problems would be given the opportunity to return after those problems had been fixed.
- Ongoing efforts to enhance the resilience of electoral infrastructure—both technical and organizational (NRC Recommendation 5.4). As technology advances, more vulnerabilities will occur and a continuing (as opposed to a one-time) effort will be needed to address them.

To address the issue of partisanship, the administration of elections should be undertaken by nonpartisan officials, and both vote casting and voter registration systems should be acquired from vendors whose senior leadership is scrutinized and demonstrably nonpartisan.[22]

2.6. Retain the designation of election infrastructure as critical infrastructure.

In 2017, the Department of Homeland Security designated election infrastructure as critical infrastructure, thus making operators of election infrastructure eligible for a variety of its cybersecurity services. Election infrastructure was defined as "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[23] The designation of election infrastructure as critical infrastructure gives priority to the systems involved as a matter of national security—quite appropriately

given the role of that infrastructure in supporting the foundations of the nation's democracy (NRC Recommendation 5.1).

2.7. Allow political parties to provide cybersecurity assistance to state parties and to individuals running for federal office and their campaigns.

Currently, Federal law (52 U.S.C. 30116) limits the amount of financial support that political campaigns can receive from national political parties. Without legislative relief, cybersecurity assistance must be treated as an "in-kind donation", and thus would count against those limits and reduce the amount of direct financial support a campaign could otherwise receive. As of the date of this writing, there is at least one bill in draft form that provides for such relief; in any case, legislation to this effect should be enacted with all due haste.

CHAPTER THREE

Regulating Online Political Advertising by Foreign Governments and Nationals

By Nate Persily and Alex Stamos

The Problem

Agents of the Russian government purchased a significant amount of digital advertising during the 2016 U.S. presidential election. The scale of the paid advertising effort and the exact amounts of foreign spending on digital ads remain unknown and may never be known. However, it is now well understood that, alongside "organic" social media content, paid advertising by Russian nationals helped push messages about candidates and issues relevant to the 2016 election campaigns.

Facebook's investigation of Russian spending on its platform, as well as the indictments and report from Special Counsel Robert Mueller and his team, provide most of what is known about Russian paid-advertising throughout the campaigns.[1] Through 470 inauthentic accounts, Russians spent over $100,000 (some in rubles) on over 3,500 advertisements on Facebook and Instagram between June 2015 and May 2017, in addition to unspecified amounts through Google and Twitter.[2] As is often true for advertisement spending even by domestic actors, the impact of these communications is hard to quantify.[3]

The online ads run by Russian organizations and agents contained a variety of messages with varying connections to the presidential campaign. Some contained explicit messages of endorsement or opposition to a candidate, containing phrases such as "Support Hillary", "Save American Muslims", "Make America Great Again!", or "Join Florida Trump Rallies". Others mentioned the candidates but did not use charged language of endorsement or opposition. According to the Special Counsel report:

> During the U.S. presidential campaign, many IRA-purchased advertisements explicitly supported or opposed a presidential candidate or promoted U.S. rallies organized by the IRA (discussed below). As early as March 2016, the IRA purchased advertisements that overtly opposed the Clinton Campaign. For example, on March 18, 2016, the IRA purchased an advertisement depicting candidate Clinton and a caption that read in part, "If one day God lets this liar enter the White House as a president - that day would be a real national tragedy." Similarly, on April 6, 2016, the IRA purchased advertisements for its account "Black Matters" calling for a "flashmob" of U.S. persons to "take a photo

> with #HillaryClintonForPrison2016 or #nohillary2016." IRA-purchased advertisements featuring Clinton were, with very few exceptions, negative. IRA-purchased advertisements referencing candidate Trump largely supported his campaign. The first known IRA advertisement explicitly endorsing the Trump Campaign was purchased on April 19, 2016. The IRA bought an advertisement for its Instagram account "Tea Party News" asking U.S. persons to help them "make a patriotic team of young Trump supporters " by uploading photos with the hashtag "#KIDS4TRUMP." In subsequent months, the IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the Facebook groups "Being Patriotic," "Stop All Invaders," and "Secured Borders."[4]

The lion's share of Russian-sponsored ads, however, did not directly reference the candidates, but instead addressed divisive political issues, including gun rights, immigration, police brutality, or terrorism. Some of these ads went so far as to encourage Americans on both sides of an argument to actively join groups or attend rallies. Judging by the content of their ad buys on social media platforms, the Russians engaged in the 2016 U.S. presidential election had two goals—support Trump by disparaging Clinton, and amplify existing polarization in American society.

These critical distinctions matter both for existing law and the constitutional restrictions that might govern certain proposed reforms. To date, digital campaign spending is largely unregulated, notwithstanding two key exceptions: (1) a ban on electioneering communications sponsored by foreign nationals and (2) disclosure requirements for all advertisements of candidate-advocacy placed for a fee on another person's website. Many of the Russian ads violated these laws, but the majority did not. To prevent similar foreign spending in future elections requires policy innovations tailored to the unique opportunities that online environment offers malicious actors and the unique challenges that this environment presents to regulatory agencies in charge of promoting transparency in campaign spending.

To successfully confront the exploitation of digital political advertising platforms by foreign actors, several significant obstacles must be overcome. In particular, the 2016 campaign revealed how the internet facilitates anonymous campaign spending and how the law's limited reach to candidate-related advocacy can be easily avoided by foreigners spending money on issue advocacy. Although serious constitutional constraints rightly limit available options, any new regulation that seeks to address the problems discovered in 2016 must deal with these two problems: anonymity and issue advocacy. Disclosure represents the necessary first step for any reform. However, capturing the relevant universe of ads deemed "political" and requiring disclosure presents serious challenges.

Similar challenges and concerns exist apart from the special case of online foreign intervention in U.S. elections. Reformers have long advocated for greater disclosure in political

advertising and greater regulation of "issue advertising". Indeed, the litigation surrounding the McCain-Feingold campaign finance law, otherwise known as the Bipartisan Campaign Reform Act (BCRA), often focused on whether the law swept in too much speech by banning corporate-sponsored advertising beyond "express advocacy" or communication promoting the election or defeat of candidates. BCRA banned corporate-sponsored advertising on "electioneering communications" or satellite communications made within sixty days of the general election or thirty days before the primary that refer to a clearly identified candidate for federal office and were targeted to the relevant electorate. In *Citizens United v. FEC*, the Supreme Court struck down that provision as unconstitutional. Because independent spending by individuals did not pose a threat of corruption and was protected by the First Amendment, the Court reasoned, similar spending by corporations from their treasury funds was equally protected. Given the dramatic result of *Citizens United*, fewer people paid attention to the part of the opinion that upheld, on an 8 to 1 vote, the law's disclosure provisions. The ultimate result of *Citizens United*, then, was suspicion of limits on spending, but general deference to disclosure.

Neither BCRA's "electioneering communication" definition, nor its disclosure provisions, cover messaging beyond candidate-related advertising. Although ads can influence voter perceptions of candidates without directly mentioning a candidate's name, regulating election-related speech beyond words or images, which refer clearly to candidates, has always proven conceptually and constitutionally difficult. In today's political climate, virtually any issue can become politicized, from general topics such as immigration and civil rights to features of daily life such as sports and entertainment. Defining ex ante a universe of "issues" relevant to elections or politics is challenging, if not impossible. Attempts to do so rely on vague phrases, such as "issues of national legislative importance", and place a great responsibility on administrators—or in the case of the proposed Honest Ads Act, on a social media platform—to define the phrase's meaning in application.

Regardless of how the universe of ads requiring disclosure or disclaimers is defined, any adequate disclosure regime must specify who is required to disclose, and how disclosure will properly reveal the identity of the person or entity behind the ad. With respect to foreign election interference in particular, the regime of disclosure must be tailored so that the true entity behind the ad, rather than a front organization or pass-through, is made public. With the exception of RT and Sputnik, Russian advertisements or internet communications during the 2016 U.S. presidential election largely operated through fabricated organizations to disguise the original identity of the advertiser.

Of course, the issue of ambiguous or non-transparent funding behind campaign ads is not new nor limited to the issue of foreign interference. So-called "dark money" is a longstanding problem that has accelerated in importance with the rise of prominent Super PACs and 501(c)(4) organizations involved with the independent funding of campaign-related advocacy. In contrast to the obligations placed on candidates and parties, the law places incomplete disclosure

responsibilities on Super PACs and 501(c)(4) organizations, allowing them either to evade disclosure for many expenditures or merely to disclose non-human entities, such as corporations or other associations. The law never requires disclosure for pure issue advocacy for any entity.

Most existing disclosure regimes fail to capture the original financial source of an expenditure. If the regulation merely requires an organization's name to be included in a disclaimer or in a filing with an election authority, then sponsors can create groups with innocuous, patriotic-sounding names, such as "Americans for America". Consequently, any system of disclosure that seeks to avoid the cloaking of money in intermediary organizations must require the identification of an individual who either manages the organization or contributes money to the organization above a certain threshold. If the disclosure is limited to the name of a corporation or association, then the actual source of the money—whether foreign or domestic—can easily remain concealed.

Finally, any regime that addresses either express or issue advocacy must have special provisions for the media. Journalists and the companies they work for spend money on "communications" that refer to candidates and have a sizeable impact on election coverage and results. Media coverage of campaigns is more ubiquitous and influential than paid online communication, such as advertisements. As compared to news and other unpaid commentary, advertising represents only a tiny share of voters' exposure to information sources relevant to campaigns. A disclosure regime, or any campaign finance regulation for that matter, that covers expenditures on politically relevant communication must draw a line between legitimate media organizations and other forms of paid communication. All existing campaign finance regulations do so, but defining the media in the age of the internet is challenging given that anyone can blog, post, or Tweet. YouTube celebrities often have followings comparable to established media organizations. Interest groups regularly create their own webpages and news-like sites in order to appear similar to journalistic institutions. Although any "media exception" for campaign finance regulation will inevitably exclude some legitimate journalists and include some illegitimate ones, the designers of such regulations need to carefully consider the impact on free speech from roping legitimate media into definitions of paid electoral communication.

Existing Proposals

Since the 2016 U.S. presidential election, social media platforms and members of Congress have explored different proposals for increasing transparency related to political advertising, particularly regarding expenditures by foreign nationals. Proposed by Senators Mark Warner and Amy Klobuchar, the Honest Ads Act[5] is the most advanced legislative proposal thus far. A similar proposal, titled the New York State Democracy Protection Act, was signed into law by Governor Andrew Cuomo in April 2018.[6]

The Honest Ads Act would require a public archive of all election-related advertisements, both candidate-related and on issues of national legislative importance. Maintained by the FEC, the

archive would contain a digital copy of the ad, a description of the target audience, the number of views or impressions, and the rate charged for the ad buy. In addition, clear disclaimers revealing the name of the organization or individual who paid for the ad would be required.

In the wake of the 2016 U.S. presidential election and in the shadow of potential legislation, several social media platforms have developed new transparency regimes for political advertising that include a similar public library of political advertising, including the ad's sponsor, frequency, and how much was spent.[7] Facebook already has created a searchable archive for all political ads—both candidate-related and those determined as on "issues of national legislative importance"—for its platform and Instagram. All ads will stay in the archive for at least seven years and include information on the number of impressions or views by gender, age, and state. Facebook users can search the archive on keywords and select ads from specific sponsors. Similarly, Google presents candidate-related advertisements in its public library. Google also notes the demographics of individuals targeted by the advertiser and the total amount spent, whereas Facebook only tracks and records the viewers themselves. In addition, Twitter's archive for political advertisements is searchable by Twitter account, as well as targeted and actual audience, including characteristics such as age, gender, language, or location by state and city.

None of these archives or libraries are optimized for the kind of research that is necessary to trace with accuracy the flows of money from outside groups to the platforms. They vary greatly in the search features they provide (especially whether ads can be organized by date) as well as the clarity with which they identify spenders. Facebook, for example, identifies spenders according to Facebook pages, which can change, as opposed to an FEC-identified account, which would be crucial both to measure legal compliance and to trace spending across platforms. Google does not provide information on political candidates' advertisements in state elections or advertisements on political issues. The shortcomings of the ad archives led a group of scholars connected to Mozilla to issue a helpful letter describing to the platforms what an effective ad archive would look like.[8]

Recommendations

3.1. Explicitly prohibit foreign governments and individuals from purchasing online advertisements targeting the American electorate and aimed at influencing U.S. elections.

The prohibition on electioneering activity by foreign nationals should be clarified to make explicit a ban on any foreign-sponsored online advertisements that target the American electorate and are intended to influence a U.S. election. The ban should apply to any advertisement that mentions or features a candidate or party within sixty days of an election, as well as advertisements on issues of national legislative importance during that time period. Because such issue ads are difficult to identify *ex ante*, the FEC should develop a list of such issues for which the ban would apply.

3.2. Support the passage of the Honest Ads Act with several key amendments.

The Honest Ads Act represents an important first step in bringing online advertising within the regulatory ambit of existing law. At a minimum, the U.S. Congress must pass and President Trump must then sign into law the Honest Ads Act to establish fair and reasonable guidelines for online advertising in political campaigns, including the regulation of foreign actors in this domain. But more could be done; this legislation could be strengthened with several amendments to more effectively increase the transparency of online political advertisements.

Currently, the most significant drawback of the Honest Ads Act is that the draft legislation places the critical responsibility of defining a political ad or an "issue of national legislative importance" entirely with the social media platforms themselves. Disclosure of issue advocacy represents a dramatic shift in the law, and it is too significant to trust private companies with defining which issues rise to the level of warranting advertising disclosure. As Facebook has moved in this direction, the firm has run into an array of line-drawing problems, including (1) addressing media organizations that boost news stories; (2) potentially designating charitable activity as political if, for example, its advertisements are related to health; or (3) managing product ads that touch on politics, such as a recent Nike ad featuring Colin Kaepernick, a Budweiser ad mentioning immigration, or an Amazon ad promoting a political book. Strong arguments could be made in favor of disclosure in all or just some of these cases, but such decisions should not depend on an individual company's definition. Instead, the Honest Ads Act should be amended to make the FEC responsible for declaring for a given election cycle what issues require ad transparency, along the lines described in the ban on foreign advertising described above.

The second drawback of the proposed legislation concerns the disclosure of targeting information. While the Honest Ads Act is premised on a conception of targeting in which advertisers specify demographic categories and/or geographic regions, targeted online advertising has moved beyond categories of users to individual lists of users. The most sophisticated political consultants and parties now curate lists of individuals, along with email addresses to identify them, so as to send individualized messages to them. These lists are then turned over to Facebook and Google who promise to deliver the advertisement to a list of people (a "custom audience") representing a large share of the targets. Moreover, Facebook also has provided "lookalike audiences", which is a Facebook audience similar to the one originally targeted. Exposing individuals' names rather than larger group-targeting categories, such as suburban white women between the age of 30 and 40, raises serious privacy issues.

Data regarding who was exposed to an ad is equally if not more important than targeting information. As targeting increasingly moves away from categories and towards individuals, advertisers or platforms cannot be expected to reveal the names of people who are targeted by the ad. "Exposure disclosure" should instead be required at a smaller level, such as zip code, census block, precinct level, or even at the county or district level. Talented enterprising analysts—and opposing campaigns—may still be able to identify some individuals from this geographical data,

but the specific characteristics of these individuals would remain concealed. Although platforms tend to balk at such micro-level disclosure because it reveals the "secret sauce" of advertisers, the innate surgical precision of effective individual-level targeting remains a key problem with digital advertising, and exposure disclosure is the only way to truly understand the dynamics of modern campaigning. At a minimum, policy makers and the platforms should consider calibrating disclosure to the level of ad targeting, in order to ensure that the more micro targeted an ad, the greater the disclosure obligation on the spender.

A third challenge with the Honest Ads Act concerns the current requirement of a library for the "creatives" or the actual advertisements delivered to targets. By combining artificial intelligence with advertising, modern campaigns in some instances have created hundreds of thousands of variations on a given ad that are A-B tested with targets. Subsequently, the platforms have taken the logical position that no matter how minor the variation, each creative is then presented as its own advertisement in the library. To maximize efficiency, however, analysts should classify advertising and spending by candidate or group, so that the library could organize creatives into groups derived from a core advertisement, and the universe of ads and their collective targets can be analyzed and evaluated more coherently.

Finally, new regulations of online political advertising provide an opportunity to address the challenge of "dark money" or front organizations that place advertisements funded by individuals and groups wishing to evade disclosure. Compared to television or other media, the internet affords greater capacity for foreign and domestic actors to participate in surreptitious activity to influence elections. By revealing the individuals who sponsor advertisements, both disclosure and disclaimers can effectively uncover the original source of the money. Therefore, advertisers and platforms should be required to disclose the names of responsible individuals and entities to the FEC, and each online ad should be identified by the FEC code of its purchaser. In practice, this recommendation would likely require, on the face of an ad or with one click-through, a list of the top five individuals who fund an organization (e.g., Super PAC), the CEO of a corporation funding ad, or the leader of a union funding an ad. Certainly, this requirement will not solve all problems, because shell corporations can be established to ensure that the CEO is not truly "responsible" for the advertisement. But this mandated change would represent a significant step in the right direction for increasing campaign transparency.

3.3. Strengthen self-regulation mechanisms for the major internet platforms.

Tackling foreign interference in U.S. elections requires new effort from both government and the private sector. The 2020 presidential campaign is already underway and most of the applicable restrictions on foreign spending come from legislation drafted in the pre-internet age. In addition, given the pace of technological change, foreign adversaries (like domestic political entrepreneurs) will always be one step ahead of any regulatory regime the U.S. Congress designs. The major internet platforms, therefore, must together confront the problem of foreign sponsored advertising, as they should foreign election manipulation through other means.

Such coordinated action may require a specific exception to the antitrust laws or a congressionally blessed industry self-regulatory body akin to the Financial Industry Regulatory Authority. However such coordination is achieved, preventing foreign interference should demand the same kind of collective industry response that was engendered by terrorist recruitment and child endangerment. In those domains, the industry has found a way to trade information and develop best practices to confront common problems. Foreign election meddling is another such issue. All efforts should be made by social media and other internet companies to present a common front against foreign election interference in the run-up to the 2020 U.S. presidential elections.

CHAPTER FOUR

Confronting Efforts at Election Manipulation from Foreign Media Organizations

By Nate Persily, Megan Metzger, and Zachary Krowitz

The Problem

Much of the analysis of Russian intervention in the 2016 U.S. presidential election has focused on covert forms of internet-based influence generated through clandestine social media campaigns and advertising. However, not all efforts by the Russian government or its affiliated entities were done in secret. Some attempts at influence were open and notorious, such as the stories broadcasted, posted, and promoted by Russian media organizations RT and Sputnik. Policy prescriptions for how the U.S. government or social media companies should confront efforts by foreign governments to influence U.S. elections through official media organizations, however, raise complex questions regarding the rights of those organizations, as well as the government's regulatory capacity to distinguish between authentic journalism, government-sponsored propaganda, and election manipulation.

As discussed in Chapter One, the Russian government created Russia Today in 2005. Although formally modeled after the BBC, RT was later renamed and evolved into an effective propaganda outlet for transmitting the values and objectives of the Russian government across the world. As the Kremlin's response to Western criticism of its anti-democratic efforts, RT uses an international, multiple-language, 24-hour television service and associated website to promote Russian policies and attack the values and policies of Western governments, especially those of the United States.[1] With a budget of approximately $300 million, RT is available on Comcast, Cox, Charter, DirecTV, and Fios, and claims that it "reaches more than 644 million people worldwide."[2] As mentioned earlier, RT also claims to be the number one watched "news" channel on YouTube.[3] Sputnik, for its part, is "a brash Russian-government-run news and commentary site that models itself on BuzzFeed."[4]

In addition to adopting a name change to obscure its connection to the Russian government, RT America operates through a complex network of financial arrangements to create fictional distance between the media organization and the Russian government. The Russian government finances RT through a parent company, TV Novosti, which in turn transfers money to a production company, T&R Productions, to underwrite RT America. This convoluted web

of funding is tailored towards demonstrating formal independence, despite clear control and financial responsibility by the Russian government. RT editor-in-chief Margarita Simonyan has spoken frequently about the instrumental role her organization plays in advancing Russian state interests, at times even implying that RT is as important to the Russian state as the Russian Armed Forces.[5] Statements from those who have left both RT and Sputnik confirm the lack of journalistic independence from the state.[6] Controversial coverage by RT of the Russian military intervention in Ukraine in 2014 resulted in one of its anchors, Liz Wahl, resigning while on-air.[7]

In some respects, however, RT and Sputnik are functionally indistinguishable from a host of similar media organizations within and beyond the United States. While the overwhelming majority of RT's stories are true, others are barely news at all, but instead clickbait used to acquire a sizeable audience. They often feature controversial figures, such as Nigel Farage when he was championing Brexit,[8] 9/11 truthers, or those who believe Osama bin Laden's death was staged.[9] Simonyan also has explicitly stated that part of Russia and RT's strategy is to build audiences through lighter entertainment shows and soft news during less volatile times, but then to target them with political messages during more critical or vulnerable moments.[10]

The U.S. intelligence community's report following the 2016 U.S. presidential election described how RT and Sputnik had "contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences."[11] RT coverage of the campaign followed what is now acknowledged as the larger Russian strategy of sowing discord, diminishing Hillary Clinton, and facilitating mixed but generally more positive coverage of Donald Trump.[12] RT and Sputnik segments focused on Clinton's health,[13] discussed alleged corruption,[14] and called her the "Queen of War."[15] Additionally, RT focused its election coverage on significantly highlighting Senator Bernie Sanders in a positive light in the primary.[16] In the general election, RT devoted considerable coverage to third-party candidates, especially Green Party candidate Jill Stein. In 2015, Stein attended an anniversary gala for RT's 10th anniversary, where she was seated at the head table with Putin. In 2016, RT interviewed Stein several times, focused considerable attention on events such as the Green Party convention, and explicitly suggested Stein was a better choice for the American left.[17] Third-party debates were even hosted on RT between multiple Green Party candidates and between Stein and Gary Johnson, who were excluded from the major candidate debates. RT was therefore a substantial source of Stein's television coverage in the 2016 U.S. presidential election.

Concrete data on RT's reach are hard to find, but circumstantial evidence suggests that RT succeeded in effectively reaching many American internet users during the campaign period. By 2017, views of its flagship channel alone were similar to CNN's, with over 2 billion views,[18] and an interview on the U.S. elections with Julian Assange in November 2016 was one of RT's most popular videos the following year, with over 2 million views alone.[19]

RT trails mainstream media considerably in terms of followers on Twitter and Facebook. While RT's YouTube viewership at times has rivaled and surpassed CNN's, RT is far behind CNN on Twitter, with 2.6 million compared to 38.1 million followers respectively.[20] And yet, in

2016 RT was the 30th most shared news source on Twitter for election-related stories,[21] placing it just below Vox and ABC News and above Time Magazine and Slate. In other words, RT's reach on Twitter was similar to sources that would be considered fairly mainstream in the United States. Although the numbers are unavailable for how many of those viewers were located in the United States, recent research[22] during the 2018 elections found RT to have a similar ranking among users geo-located in the United States, putting its reach just between Vox and The Huffington Post in the week before the midterms.

RT and Sputnik pose difficult conceptual and regulatory challenges for U.S. government officials and executives at social media companies who seek to reduce Russian influence over the American electorate. And more generally, well beyond these specific Russian media organizations, distinguishing good from bad actors and manipulation from quality journalism presents intractable line-drawing issues that no regulatory regime can specify *ex ante*. In addition, the U.S. treatment of foreign media organizations generally and Russian companies in particular cannot be considered in a vacuum. As discussed in detail in Chapter Seven, when the United States seeks to promote democracy worldwide, some foreign governments accuse the American government of meddling in their internal affairs. Therefore, active U.S. regulation of foreign media organizations targeting American audiences could trigger retaliation in Moscow and elsewhere against both publicly sponsored (e.g., Voice of America or Radio Free Europe) and private U.S. media entities. Russia already has taken steps to retaliate against several U.S.-based media organizations by labeling them as foreign agents.[23]

In considering reform measures to address foreign election manipulation, it should be recognized that the "foreign-ness" of a media organization exists along a continuum, and is often far from a black and white distinction. At one time, for example, News Corp, which owned Fox News, The New York Post, and the Wall Street Journal, was an Australian corporation and had an Australian CEO, Rupert Murdoch, who later became a U.S. citizen. The Korean Unification movement leader Sun Myung Moon founded The Washington Times, which was owned by a corporation he had founded until 2010. Additionally, WikiLeaks transmits a sizeable amount of content in the United States, but has been registered as a library in Australia, a foundation in France, and a newspaper in Sweden, in addition to using two U.S.-based non-profit 501c3 organizations for funding purposes.[24]

Further along the spectrum, foreign governments own or control many international media organizations based outside the United States, such as RT with its well-established connection to the Russian government. A variety of media organizations, however, exist with less direct connection to foreign governments and with greater or lesser connection to the United States. Should BBC America be treated differently than BBC, for example? Should RT be treated differently than the BBC, Deutsche Welle (DW), France24, China Central Television, or Al Jazeera? Moreover, the conceptual and regulatory challenges become increasingly complex in the online environment, given the multiplicity of online sources of news, as compared to the limited number of broadcast and cable stations. Even defining or characterizing a news or media

organization for the online environment has proven difficult, let alone the degree of foreign ownership or influence over organizational operations that lead it to cross a legally relevant line drawn to identify foreign media sources.

Assuming the law can identify the requisite degree of "foreign-ness" of media outlets, the question of delineating propaganda and election manipulation from standard news or campaign coverage remains. RT does present "news", as well as what is sometimes described as "disaster porn", referring to viral stories of natural disasters, criminal incidents, and bizarre mishaps. In between these stories, which help develop its audience, RT weaves in opinion that promotes Russian government policy. RT is distinctive, not because of the unique substance of its coverage, but because of the identity of its sponsor, its intent, and its role as an instrument in pursuing Putin's foreign policy objectives. Because of its mix of news and propaganda, however, it poses a unique challenge for First Amendment law. Foreign governments or their agents are not protected by the First Amendment, but a law that might ban such media from internet platforms accessible to an American audience would pose unprecedented constitutional questions. As dangerous or effective as foreign sponsored propaganda might be, it will be difficult, as a constitutional matter, to control Americans' access to such communication on the worldwide web.

Recent Measures and Existing Proposals

In response to Russian election manipulation efforts in 2016, the U.S. government compelled RT and Sputnik to register under the Foreign Agents Registration Act (FARA).[25] FARA was passed in 1938 in response to a large group of American non-citizen residents being paid to disseminate propaganda on behalf of foreign governments and parties, including the German Nazi Party.[26] Initially, FARA required "each agent of a foreign principal to register with the government and disclose certain information," but it did not limit expenditures by those agents.[27] In 1966, Congress amended FARA "to prohibit any person acting under the direction or control of a foreign principal from knowingly making any contribution 'in connection with an election to any political office.'"[28] FARA defines an "agent of a foreign principal" as "any person who acts as an agent, representative, employee . . . or any person who acts in any other capacity at the order . . . of a foreign principal" who also engages in political activity for the foreign principal in the United States or "acts within the United States as a public relations counsel, publicity agent, information-service employee or political consultant for . . . such foreign principal."[29] The law exempts any newspaper, press service or association organized if it is at least 80% owned by American citizens of the United States, and the policies are not controlled, financed, or otherwise determined by a foreign principal.[30]

FARA requires foreign agents to register with the Attorney General[31] by disclosing the agent's name, a description of the agent's business, and any actions taken "as an agent of a foreign principal", the "nature and amount" of contributions given by the principal to the agent in the last sixty days, written and oral agreements between the agent and principal, a "detailed statement

of every activity which the registrant is performing for anyone other than a foreign principal . . . which requires registration" under FARA, and "[s]uch other statements, information, or documents pertinent to the purposes" of FARA.[32] The law then bars foreign agents who transmit "informational materials" to do so "without placing in such informational materials a conspicuous statement that the materials are distributed by the agent on behalf of the foreign principal."[33] Furthermore, the law requires every foreign agent to "keep and preserve . . . books of account and other records with respect to all his activities" that can be inspected by U.S. Justice Department officials.[34] Thus, FARA currently has three different requirements for foreign principals: registration, disclosure, and record keeping.[35]

Prior to 1995, FARA referred to political propaganda, rather than informational materials. It considered political propaganda to be communication that is reasonably adapted to indoctrinate, convert, or in any other way influence a recipient with reference to the political or public interests, policies, or relations of a foreign government or political party.[36] When faced by a First Amendment challenge to this seemingly vague provision, the Supreme Court nevertheless upheld the definition of propaganda, a decision that remains important for considering contemporary reform options.[37]

Before the government forced RT and Sputnik to register under FARA, only the media organizations NHK Cosmomedia and China Daily had been previously required to register.[38] Not surprisingly, RT opposed the FARA designation, arguing that the law's disclosure obligations would interfere with its journalism, for example by requiring the disclosure of confidential sources. Nevertheless, the U.S. Department of Justice required RT and Sputnik, as well as RT's parent company T&R Productions, to register as foreign agents.

In its FARA filing, T&R Productions noted that "the Russian Federation finances ANO TV-Novosti [the nonprofit, nongovernmental organization that oversees RT] to a substantial extent."[39] In its press release about the registration of T&R Productions as a foreign agent, the U.S. Justice Department wrote that T&R registered "as an agent for ANO TV-Novosti, the Russian government entity responsible for the worldwide broadcasts of RT Network."[40] Moreover, Acting Assistant Attorney General Dana J. Boente explained the move as an attempt to show Americans "who is acting in the United States to influence the U.S. government or on behalf of foreign principals."[41] Because T&R was ultimately labeled a foreign agent, RT lost its credentials for covering Congress-related news.

Independent of U.S. government action, social media platforms have taken several measures to reduce the reach of Russian government-sponsored media. In October 2017, Twitter announced that RT and Sputnik will no longer be allowed to advertise on the platform.[42] The company also pledged to use previously earned revenues from these organizations to fund research on the 2016 U.S. presidential election.[43] Google and YouTube also have begun to provide context when results from RT are displayed. Below all RT videos, YouTube currently states, "RT is funded in whole or in part by the Russian government" and provides a Wikipedia link with more information. YouTube has started to include similar disclaimers for other foreign-sponsored media

organizations as well, albeit with slight variations. For example, BBC videos are accompanied by the message "BBC is a British public broadcast service." In addition, after announcing the "deranking" of RT and Sputnik in its search results in order to combat misinformation, Google removed RT from its preferred news lineup, a group of news providers who receive access to additional revenue from premium advertisers.[44] Facebook recently suspended several pages linked to RT and demanded a disclosure of affiliation, citing the need for users "connecting with pages [not to] be misled about who's behind them."[45]

Recommendations

Less democratic governments would likely respond to the challenge posed by RT by banning it from the airwaves and blocking it on the internet altogether. For the same reasons justifying the registration of RT under FARA, the United States government may have the authority to do so as well. But banning RT and Sputnik would present constitutional questions concerning the right of American audiences to hear and view content from foreign media entities. An outright ban of these Russian propaganda agents also would likely trigger retaliation against legitimate, independent American media companies in Russia and other autocracies around the world. Short of a direct ban, therefore, we recommend a series of disclosure measures by social media platforms and the U.S. government as a strategy to help temper and mediate the most aggressive propaganda efforts of foreign media organizations.

4.1. Require greater disclosure measures for FARA-registered foreign media organizations.

Foreign media organizations registered under FARA should be required by law to present disclaimers attesting to their registration as a foreign agent. In practice, this restriction could include a disclaimer at the bottom of RT broadcasts and internet videos that simply identifies the station either as an "agent of the Russian government" or "sponsored by the Russian government". The same should be required, to the extent possible, for online texts and images. This regulation should apply specifically to the foreign agent itself, but it could also apply, if practicable, to the cable provider or platform hosting the content.

4.2. Mandate additional disclosure measures during pre-election periods.

If requiring foreign agents to disclose their FARA registration all the time is deemed too speech-restrictive, then more minimally, all foreign media organizations registered under FARA should be obligated to run such disclaimers in pre-election periods. As with the electioneering restrictions under the Bipartisan Campaign Reform Act, the pre-election period could be defined as sixty days before the general election and thirty days before the primary. Because these periods are when foreign-sponsored propaganda are likely to have the most electorally-relevant impact and damaging influence, clear signals for the broadcast's origin and likely intent of its sponsor can help viewers contextualize the presented information.

4.3. Support existing disclosure measures of specific social media platforms.

Companies such as YouTube, Twitter, and Facebook should voluntarily adopt measures—as some already have done—to promote these disclaimers to the extent possible. Undoubtedly, much of the content promoted by RT, Sputnik, or similar organizations will appear on the internet without disclaimers, particularly when forwarded by individual users or retweeted. Propaganda efforts can be mitigated by tagging the shared content with similar disclaimers, at least during the pre-election period. Moreover, steps to demote content by FARA registrants and prohibit their advertising (even nonpolitical advertising and "boosting" of posts) in the pre-election period should be encouraged.

If such a body of law and practice were to be developed as a supplement to FARA registration, the stakes of being labeled a foreign agent would become much higher, and thus, the United States could expect more intense objections to such designations, as well as an increase in retaliatory measures against American media organizations. Nevertheless, with respect to broadcasting to their own populations, authoritarian and semi-authoritarian regimes are quick to do much more than force disclosures on U.S. media organizations, even in cases without cause or evidence. As an example, both Voice of America and Radio Free Europe/Radio Liberty have only recently been labeled foreign agents in Russia, but have been "banned from broadcasting in the country since 2014 and 2012, respectively."[46]

As regulations expand beyond designating media organizations as foreign agents to monitoring foreign media organizations in general, the potential sweep would be quite broad. However, as foreign propaganda efforts through official government-sponsored media—whether from Russia, China, or anywhere else—become increasingly common, it may be necessary to adopt a bright line of disclosure during the pre-election period for foreign media organizations, irrespective of FARA registration. If such efforts become warranted, then even foreign media organizations that do not engage in propaganda activities on par with RT also might be required to run disclaimers indicating that the channel, video, or news item comes from a source supported by a given foreign government.

The abovementioned recommendations for regulation cannot fully prevent foreign-sponsored content from appearing on the internet or influencing American voters during election and non-election periods. "Information wants to be free", as the old adage goes, and content from international sources will continue to make its way onto American screens regardless of security efforts. Nonetheless, disclaimer regulations can serve the crucial purpose of un-packaging RT from the seemingly innocuous brand name it has adopted. Foreign instruments of state propaganda will continue to seek to influence the American electorate. Therefore, foreign agents should always be identified as what they are and where they come from. Whether the transmitted propaganda will ultimately persuade the American voter presents a challenge to democratic theory and decision-making—one that law in a free society may be incapable of preventing comprehensively and effectively.

CHAPTER FIVE

Combatting State-Sponsored Disinformation Campaigns from State-aligned Actors

By Alex Stamos, Sergey Sanovich, Andrew Grotto, and Allison Berke

The Problem

As documented in great detail in the Special Counsel report, the publication of stolen documents, purposively provocative and divisive misinformation, and disinformation dissemination through social media platforms by Russian government agents and their proxies constituted one of the most impactful methods of Russian government interference in the 2016 U.S. presidential election. Social media companies were unaware of the scale and scope of the malicious activities happening on their platforms as they occurred, and downplayed the potential impact for too long. Eventually, after significant pressure and criticism from lawmakers and the press, the companies began to take action. The U.S. government, and the FBI in particular, also did not communicate in a timely manner with social media companies about information they were collecting on Russian disinformation operations. Cooperation between the public and private sector on disinformation was almost non-existent before the 2016 U.S. presidential election, a situation that has improved only slightly since.

Several social media companies have taken measures to reduce the influence of foreign-government content producers on their platforms. Google, Facebook, and Twitter have created teams to find and shut down organized disinformation actors, although these shutdowns have not always been publicly disclosed. One known operation against Russian groups occurred in April 2018 when Facebook's team removed 70 Facebook accounts, 65 Instagram accounts, and 138 Facebook pages controlled by the IRA.[1] Additional takedowns of a variety of actors, including accounts operating from Iran, Pakistan, and India, have followed.[2]

As highlighted in Chapter Three, the most tangible progress in preventing online disinformation to date has been restrictions on the use of paid advertisements to spread disinformation on social media platforms. For instance, in the summer of 2018, Facebook, Twitter, and Google implemented new requirements for political ads, including ads on "social issues", to be labeled with "Paid for by" disclaimers. In the United States, these ads can only be run by verified residents of the U.S. and are stored in public archives along with particular targeting and reach data. Anecdotal evidence suggests that this approach may deter certain known players

in information warfare. For example, In the NOW, a video-focused RT outlet with over 3 million Facebook followers, attempted to run an advertisement on the site in early June 2018 for its story on poverty in America, but the advertisement was removed due to its lack of a "Paid for by" label. Deciding not to disclose the source of its funding, In the NOW chose to not run further ads before being banned outright in February 2019.

The ban and its subsequent reinstatement also illustrate the inconsistent implementation of labeling across platforms. While In the NOW videos on YouTube were being labeled as "funded in whole or in part by the Russian government," the same videos on Facebook were not. After a CNN report, the page was banned by Facebook, then required to reveal its source of funding under a new policy, then reinstated. The entire process was closely covered by both Russian and American media, which ultimately raised the page's profile and popularity while rendering Facebook vulnerable to censorship charges.[3]

To successfully combat state-sponsored disinformation campaigns, further efforts must be undertaken. In part, the solution requires implementing previously adopted solutions in a more comprehensive and coordinated manner, particularly with regards to paid content and advertising on social media.

A second line of work must focus on improving tools and strengthening policies to support efforts to identify and neutralize existing and emerging types of organic content used for disinformation purposes, as well as hacked or leaked documents. In addition to the recommendations provided in Chapter Three regarding the regulation of paid advertisements from foreign-government content producers, additional measures should be taken to reduce the impact of disinformation and stolen material spread from foreign government-aligned actors seeking to influence American voters. Most of these actions could be taken by private companies and need not be mandated through government regulation or new laws.

Moreover, legal and cultural changes need to be made to enhance cooperation between social media companies and between the private sector and the government to thwart disinformation campaigns. Tackling this issue involves addressing the larger question of data privacy. After a series of privacy scandals over the last several years, consumers justifiably want greater accountability from the companies that hold their private data, especially when this data might be used to influence their voting preferences. The U.S. Congress has started to debate the contours of a new federal consumer privacy law, prodded in part by California's consumer privacy law passed in 2018.[4] Tradeoffs between privacy and safety will frame this debate, which should include discussions of which parties are responsible for certain areas of election protection and what data are necessary for them to fulfill those responsibilities.

Social media companies will be far more effective against disinformation campaigns if they can coordinate and cooperate, and if they can partner with other large journalistic outlets to agree on norms around spreading and citing manipulated or stolen content. To do so, however, requires that information sharing about these threats be lawful. For example, it is debatable how

information posted publicly but subsequently taken down by a platform should be handled under the Electronic Communications Privacy Act (ECPA).

Exceptions to privacy requirements should be just that—exceptional. On the other hand, if the U.S. Congress wants to incentivize private companies to take more action against disinformation, it may have to pass new legislation to lower or eliminate those legal barriers now in place for doing so.

Recommendations

5.1. Create standardized guidelines for labeling content affiliated with disinformation campaign producers.

Social media companies and other online platforms need to develop and publicize industry-wide guidelines for labeling content from producers engaged in disinformation and information warfare. They also need to maintain a database of entities, which are actively employed in delivering disinformation. While the link between RT and In the NOW was never concealed, it is likely that under increasing pressure, future producers of disinformation will become progressively adept and creative in hiding their true identities.

A good initial step would be unified standards and language around government-aligned or government-sponsored media. Care would have to be taken to avoid false equivalence between outlets, which are editorially independent from governments but receive funding from them, such as the BBC and PBS, and outlets more closely aligned with their governments' policies, such as RT and the Xinhua News Agency. An appropriate labeling regime that applies to individual pieces of content would inform users of the source of information without unduly harming legitimate journalistic outlets with government ties.

5.2. Create norms for the media's handling of stolen information.

A significant component of the GRU's portion of the Russian campaign was the manipulation of the U.S. mass media, most notably well-respected print and television news outlets.[5] This manipulation occurred both in private via emails and private messages to reporters,[6] and in public via mass dumps of stolen information.

Previous industry-wide norms of ethics and conduct have been established for media and news organizations to avoid publishing material that is truthful but that could result in violence, gratuitous emotional harm, and other disproportionate harms. For instance, most media outlets currently do not publish photos of military casualties, the names of crime victims whose next of kin have not been notified, detailed descriptions of suicide methodologies, or the names of mass shooting suspects who were motivated by notoriety.[7] To date, journalists and media executives have taken the initiative to define, coordinate, and enforce these norms.

These same actors, not the government or lawmakers, should take the initiative regarding this new frontier of ethical behavior and endorse new norms around hacked documents and other content that has been leaked for political purposes. This norm should hold in particular when

journalists believe that intelligence services or organized groups are behind strategic leaks. To be sure, leaked information is a key component of journalism that brings accountability to powerful actors. But norms around the amount of coverage given to strategic leaks, the fact-checking that goes into stories, and the context in which leaks are reported—including the source of the leak—can reduce the chance that responsible media outlets will be used by autocrats to undermine democracy.

Because journalistic reporting and social media platforms are amplification tools for disinformation and for leaked documents, the absence of their cooperation will pose a serious challenge to malicious actors in reaching a broad audience with their preferred narrative. Furthermore, the precedent of previous norms intended to protect victims or potential victims can be easily used to lend credibility to the need to protect hacking victims and subjects of manipulated content like deepfakes. Although the relationship between the American major media and multinational social media organizations is often strained, synchronizing responses to U.S. adversaries should be possible and could be determinative of whether a future attempt along the lines of DCLeaks is effective.

5.3. Limit the targeting capabilities for political advertising.

Social analytics and advertising tools serve as a "finely tuned disinformation machine for the precision propagandist."[8] Of all of the opportunities for message amplification provided by the major social media products, advertising poses the greatest risks. First, it allows for amplification limited only by the budget of the attacker. Second, it allows an information warfare actor to put content in front of citizens who did not ask to see it. Most importantly, online advertising platforms allow adversaries to target individuals and groups that are most vulnerable to their specific message. Such targeting played a key role in the IRA's audience building campaign.

While there are equivalent capabilities for individualized targeting with more traditional campaign techniques, such as direct mail, the combination of low per-unit cost and the ease of targeting online creates a need for online political ads to be monitored more aggressively. The social media companies have already created voluntary standards for defining political advertisements; they can and should voluntarily choose to limit targeting capabilities for those ads as well. The current standards have been created by a handful of large companies; existing self-regulatory groups such as the Internet Advertising Bureau[9] should be utilized to establish standards that apply to the thousands of companies involved in the internet advertising ecosystem. With or without external interference, it is important for the health of American democracy that malicious actors be limited in their ability to target very narrowly defined subgroups of Americans with advertising specifically designed to appeal to a unique concern or base instinct.[10]

5.4. Expand transparency for paid and unpaid political content.

Several large online advertisers already have created online archives for political advertisements. These archives can be improved in several ways, such as by updating the archives in near-real time and providing detailed engagement metrics.[11] This information needs to be available through an open application programming interface (API).

Social media companies also should create content archives and disclose audience information for known disinformation actors and hacked documents. Preferably, social media platforms could provide access to this information and other data through an API meeting basic standards of thoroughness, transparency, and timeliness.[12] Facebook already provides much of the relevant information via its commercial social media data offering, CrowdTangle.[13] Unfortunately, the usefulness of this platform is undermined by the immediate removal of violating content. This approach could help not only to guide fact-checkers and other counter-disinformation efforts, but also to identify the trends and, more importantly, the goals and targets of disinformation.

Existing transparency measures have been voluntary, and only a handful of companies are providing any transparency into online political ads. The U.S. Congress needs to act to set compulsory standards for online ad archives and to create a privacy safe harbor for tech platforms to share content from disinformation actors with responsible researchers.

5.5. Improve the quality and scope of detection tools and reporting policies for social media platforms.

Social media companies should also develop additional tools and formats to identify disinformation and hacked content more rapidly and remove it with higher precision, removing content before harm is done. To achieve this objective, they should draw on existing academic research in the area[14] and make the tools they develop open for verification and oversight.[15] Social media and content platforms also need to strengthen their investment in developing technology to detect new and different ways in which entities are disseminating disinformation, such as peer-to-peer messaging apps, or using machine learning-written text and inauthentic pictures, audio, and video, including deepfakes. Hosting providers with significant traffic or business operations in the United States can be incentivized to remove disinformation and hacked documents upon coordination with law enforcement and victims, similar to measures that are taken to remove explicit sexual content or copyright-infringing content. Establishing regular searches for, and removal of, this content will disrupt channels that hackers use to disseminate leaked documents, and will provide the perception that this content, in the few places where it can be found, is untrustworthy or potentially discrediting to host or possess. It is therefore critical to enforce industry-wide norms or legislation with regard to this issue.

As we have witnessed already, when social media platforms institute policies that could result in the removal of user content, they must be mindful of the high costs of false positives, i.e., unjustified removals. This error matters not only with regards to freedom of expression from the individual user's point of view, but also as a factor of legitimacy for the justified removals. Platforms, therefore, cannot rely on artificial intelligence (AI) alone, but must employ competent moderators—who are familiar with the local environment and know the language they are working with—as well as establish efficient appeal procedures. Instead of making these decisions inside a black box, social media platforms should provide transparency for the reasoning behind these decisions, perhaps assisted by third-party councils. This openness and clarity will help both personal and institutional users navigate relevant rules and build trust in the platform's decision-making.[16]

To both increase public awareness of disinformation threats and improve the accountability of social media platforms, platforms must develop policies for disclosing their ongoing disinformation campaigns, as well as producing regular "community health reports", including statistics on the percentage of anonymous, inauthentic, and automated accounts active in the system, and engagement metrics for the categories of accounts relative to authenticated human activity and labeled bots.[17]

5.6. Build an industry-wide coalition to coordinate and encourage the spread of best practices.

As major social media platforms become more serious about policing their platforms, disinformation may move to smaller, less prepared, and more niche platforms. Major tech companies therefore must make tools and best practices on fighting disinformation available to these less equipped companies. Moreover, the implementation of these best practices should be tied to the ability to access other important industry-wide resources such as those used to identify copyright infringement or other forms of harmful content.

There have been several successful examples of this kind of coordination. The first is the model known as the Information Sharing and Analysis Center/Organization (ISAC/ISAO).[18] These are industry-wide, non-profit organizations that provide various levels of services to their members, ranging from facilitating discussions and lightweight information sharing to operating completely independent and well-staffed intelligence functions. While the Multi-State ISAC has been an important component of securing election systems, there is no designated ISAC or ISAO for the consumer internet companies and no natural home for coordination on measures meant to prevent online disinformation.

The major companies, namely Google, Facebook, and Twitter, have a responsibility to create such an organization and to utilize it to encourage sharing among themselves, with smaller competitors to help build their capacity, and with government agencies when appropriate under the law.

5.7. Remove barriers to the sharing of information relating to disinformation, including changes to privacy and other laws as necessary.

Signed by President Obama in December 2015, the Cybersecurity Information Sharing Act (CISA) of 2015 reduced legal barriers to sharing cybersecurity threat indicators among technology companies, and between the private sector and the U.S. government, by establishing a blanket exception for such sharing under American privacy and surveillance laws. Although CISA does not require or guarantee that private companies share the information, it eliminates numerous legal constraints as a barrier to action.

As social media platforms, civil society, and government work to address disinformation threats, they should consider whether similar exceptions are necessary in order to effectively counter these threats. When conducting information operations, adversaries routinely exploit multiple platforms to disseminate their malign content. Because action by one platform to address malign content does not guarantee that other platforms become aware of the threat, the content typically persists, which enables the adversary to adapt their strategies in order to better evade future detection.

At the moment, access to the content used by disinformation actors is generally restricted to analysts who archived the content before it was removed or governments with lawful request capabilities. Few organizations have been able to analyze the full paid and unpaid content created by Russian groups in 2016, and the analysis we have is limited to data from the handful of companies who investigated the use of their platforms and were able to legally provide such data to Congressional committees. Congress was able to provide that content and metadata to external researchers, an action that is otherwise proscribed by U.S. and European law.[19]

Congress needs to establish a legal framework within which the metadata of disinformation actors can be shared in real-time between social media platforms, and removed disinformation content can be shared with academic researchers under reasonable privacy protections.

5.8. Establish a Social Media ISAC/ISAO to improve communication between the U.S. government and social media companies about disinformation operations.

Before 2020, the U.S. intelligence community must implement plans to assist social media companies in thwarting disinformation and influence campaigns from foreign governments through rapid declassification of technical indicators and regular updates on potential threats. Social media companies must be willing to engage as well with the U.S. government. Tighter coordination between U.S. agencies and tech platforms might be facilitated by third-party oversight, which would enhance the credibility of these interactions.

The U.S. tech industry currently lacks a coordinating body to facilitate data sharing and provide a single interface to U.S. agencies working to protect our elections. These companies need to create such a body, following the model of effective coordination centers already

established by the finance and power industries.[20] A new organization representing all social media companies could then act as an intermediary between the tech industry and the intelligence community for discussion of these national security issues.

5.9. Increase overall transparency on social media platforms.

More generally, social media platforms need to provide more transparency for their users in cases when content was produced or promoted using automation or AI tools. Existing user interface features and platforms' content delivery algorithms need to be utilized as much as possible to provide contextualization for questionable information and help users escape echo chambers. In addition, social media platforms should provide more transparency around users who are paid to promote certain content.

One area ripe for innovation is the automatic labeling of synthetic content, such as videos created by a variety of techniques that are often lumped under the term "deepfakes". While there are legitimate uses of synthetic media technologies, there is no legitimate need to mislead social media users about the authenticity of that media. Automatically labeling content, which shows technical signs of being modified in this manner, is the minimum level of due diligence required of the major video hosting sites.

Bots that attack other users (trolling bots) and hijack coordination tools to render them ineffective (dumping bots) have received the most attention thus far. But bots that amplify certain messages and cheerlead certain users must be carefully analyzed as well for having a serious negative impact on our elections.[21] In particular, social media platforms need to prevent bots from "following", "liking", "sharing", and "retweeting" to ensure that only organic human activity is reflected in various measures of popularity, authority, and influence on social media.

5.10. Carefully balance platform responsibility with individual freedoms.

The U.S. Congress also should consider new guidelines on the obligations of major social media platforms to their users regarding freedom of expression. Because demotion, shadow bans, and outright bans of certain kinds of content are already becoming the subject of litigation, continued efforts to resist disinformation campaigns are likely to provoke further legal disputes.

Several groups have proposed changes to the critical protections provided by Section 230 of the Communications Decency Act. The U.S. Congress needs to carefully balance the need to protect the freedom of speech and the integrity of social media platforms while also defending the country from disinformation campaigns. A good first step would be legislation encouraging transparency on how social media companies interpret their own guidelines, and standardized reports on content moderation statistics.

5.11. Establish a norm among candidates to not use stolen data or manipulated content.
Prodded by the Daily Beast in February 2019, candidates running for the Democratic Party nomination for the 2020 U.S. presidential election have pledged not to use data about other candidates obtained illegally.[22] This norm should be codified in a formal document drafted by the Democratic National Committee and then signed by all candidates. The Republican National Committee should do the same for its candidates in 2020, including President Trump.

5.12. Emphasize digital literacy in educational curricula and focus public education on the knowledge that makes democracy more resilient to disinformation campaigns.
Many of the most successful disinformation campaigns, including the one perpetrated by the Russian government against the United States in 2016, involved technically trivial, easily preventable hacking of private data. The amount of sensitive data that could be easily weaponized by a disinformation campaign will only increase and will be located far beyond the electoral campaign headquarters, including across various government and corporate entities that routinely store the personal data of millions of their patrons and clients. Building a robust defense against high-end attacks on the most critical platforms is essential, but raising awareness and developing skills among much larger groups of people who will manage people's data is also urgent. Equipping the general public with common sense digital safety skills will further increase the costs and reduce the agility of any attack.

The most powerful weapon against a disinformation campaign is a public that is curious about the sources of information, can assess their credibility,[23] and most importantly, is capable of thinking critically about the information received.[24] This means that narrowly defined digital and media literacy could serve only as the foundation for the educational programs that need to teach how to put information in context and perspective. To effectively confront disinformation campaigns perpetrated by autocracies against democracies, a teaching curriculum needs to build on serious theoretical and empirical work that uncovers the role of information in both modern autocracies[25] and democracies.[26] Emerging research in this area points to emphasizing the difference between the political and policy outcomes of the democratic process (which are legitimate goals in electoral competition) and the universal right of people and coalitions of people to participate in it (which is supposedly sacred but might require additional training to be perceived as such).[27]

To this end, the U.S. Congress should mandate the Department of Education to convene a task force on making existing[28] and new information security and media literacy curricula available to educational programs at all levels, from the primary education to lifelong learning, including tailored versions for keepers of personal data in the commercial sector, government employees, PR professionals, and other critical groups, as well as teachers who will teach these skills. The

task force should provide its recommendations following an open and transparent process of public consultation, meeting with educators at all levels and engaging different communities at the state and local level by offering opportunities to run pilot programs, whose results would undergo rigorous evaluation. To ensure that the best-performing curriculum is selected at the national level and students' progress is monitored, media literacy would need to become a part of national standardized testing as well as comparative studies such as PISA.[29]

Because empirical research suggests that older Americans are particularly vulnerable to fake news on social media,[30] public education in this area cannot exclusively focus on the younger generation currently in school or college. The task force would need to assess existing research in this area and develop, in collaboration with academic and civil society stakeholders, learning tools suitable for older audiences who are already in the workforce or in retirement.

CHAPTER SIX

Enhancing Transparency about Foreign Involvement in U.S. Elections

By Michael McFaul, Andrew Grotto, and Alex Stamos

The Problem

Our Founding Founders worried a lot about possible foreign meddling in the domestic affairs of the new United States of America. In particular, they were concerned that powerful European actors would use their wealth to corrupt elected officials in the new American democracy.[1] The Federalist papers are filled with expressions of concern about foreigners exercising influence over the conduct of American politics. More specifically, the Emoluments Clause was included in Article I of the Constitution precisely to reduce foreign influence over elected officials, declaring "no Person holding any Office of Profit or Trust under them, shall, without the Consent of the Congress, accept of any present, Emolument, Office, or Title, of any kind whatever, from any King, Prince, or foreign State."

Over time, concern about foreign influence in American politics and elections has varied, sometimes with negative results for democratic practices. The Alien and Sedition Acts were signed into law by President John Adams in 1798 in the context of undeclared armed hostilities with France, ostensibly to protect against French interference, but were used by the government to suppress political dissidents until the relevant portions of the law expired in 1800. In the run up to World War II, Congress passed the Foreign Agents Registration Act in 1938 in response to growing Nazi influence in the United States, a law that has served to enhance transparency regarding foreign lobbying efforts, but also, some believe, invoked to criminalize legitimate interactions between foreigners and Americans.[2] And most certainly, fears of foreigners meddling in American politics spun tragically out of control during World War II when Americans of Japanese descent were rounded up and forcible removed to internment camps or when Senator McCarthy launched his crusade against alleged American communists. In seeking greater transparency about foreign influence in our elections, we obviously must avoid repeating these tragic chapters in American history.

The involvement of foreigners—Russian government agents in particular—in the 2016 U.S. presidential election did expand substantially compared to recent other presidential elections.

The Mueller Report documented in detail a vast range of contacts between Russian officials, Russian business people, and Russian non-governmental leaders with American officials involved directly or indirectly in the Trump campaign. Most strikingly, Russian government officials and their proxies aggressively pursued contacts with as many Trump campaign officials as they could make, oftentimes with successful results. As discussed in Chapter One, some of these meetings involved direct offers of assistance to the Trump campaign, offers that would have worried our Founding Fathers. According to one careful count, "Donald J. Trump and 18 of his associates had at least 140 contacts with Russian nationals and WikiLeaks, or their intermediaries, during the 2016 campaign and presidential transition...."[3] Notably, the Kremlin and WikiLeaks–also a foreign non-governmental organization–showed no interest in pursuing meetings with the Clinton campaign.

Another kind of foreign involvement in the 2016 U.S. presidential election involved prospective business deals with American candidates, including Donald Trump in particular. As illustrated in Chapter One, during the 2016 presidential campaign, Trump and his colleagues actively pursued a major business deal in Russia—the construction of a Trump Tower in Moscow—and deliberately hid these negotiations first from voters and later from investigators on the Special Counsel team at the U.S. Department of Justice. The full extent of other business ventures with foreigner partners by either the Trump or Clinton campaigns—or any campaign in recent memory, for that matter—has not been disclosed.

In addition to in-person meetings, several foreign companies and consultants were paid to participate in the 2016 U.S. presidential elections. The Trump campaign hired a British firm, Cambridge Analytica, to work directly for their organization. Other Republicans candidates hired the British firm, Orbis Business Intelligence, to collect compromising materials on Trump relationships with Russian individuals and organizations. When these Republicans dropped out of the race, the Clinton campaign contracted with the American company Fusion GPS to collect opposition research on Trump, and Fusion GPS in turn hired again Orbis Business Intelligence to continue its research on Trump, a contract that eventually produced the "Steele Dossier".[4] As documented in the Special Counsel report, people close to the Trump campaign also interacted directly with another foreign organization, WikiLeaks, allegedly to coordinate the dissemination of compromising materials on candidate Clinton and her campaign.

Foreigners also made illicit donations to the Trump inauguration committee. For example, political consultant W. Samuel Patten plead guilty in 2018 to steering $50,000 from a Ukrainian politician to the inaugural committee.[5] In addition, it was reported that weeks after being placed on notice by watchdog groups, the Trump campaign had continued to solicit illegal donations from foreign individuals—including members of foreign governments at their official email addresses.[6]

Many of these contacts clearly stretch the boundaries of propriety, and several of them were considered illegal, but to date, no American has been charged with conspiracy regarding

foreign contacts during the 2016 U.S. presidential campaign. In fact, most of these contacts were legal—but should they be? Our answer is no. But even if not legally criminalized, the American voters have a right to know about presidential candidates' business and political activities with foreign individuals and companies before they go the polls on Election Day. Consequently, greater transparency is needed to ensure that voters will be able to make informed decisions for themselves about the appropriateness of these contacts and business deals with foreigners.

Recommendations

6.1. Mandate transparency in the use of foreign consultants and foreign companies in U.S. political campaigns.

Foreign consultants and companies seeking to provide advice or assistance to candidates should be required to register with the Federal Election Commission, with criminal and civil penalties for failing to register. In addition, candidates should be required to disclose their use of foreign consultants and foreign companies in political campaigns. The U.S. Congress should mandate these requirements in legislation.

6.2. Increase transparency about foreign business interests.

Candidates should not be forced to divest from all investments abroad or business deals with foreigners and their companies. Instead, candidates should make public their business interests abroad and then let the voters decide whether there are conflict of interests. The easiest way to make such information available to the voters would be for candidates to publish their tax returns. The U.S. Congress should mandate this practice in legislation.

6.3. Disclose contacts with foreign nationals and governments.

Beginning in 2020, all non-incumbent presidential candidates should pledge to document all meetings and other substantive interactions with foreign nationals, especially foreign governments, and to make public this information. To incentivize transparency, the U.S. Congress should establish information handling guidelines, including a tailored exemption for this information under the Freedom of Information Act. Many government agencies already require such disclosures, and the same practice should apply for campaigns. The significance of requiring candidates and their campaign officials to report contacts with foreign nationals attempting to coordinate, make campaign donations, or offer information and services is echoed in the Foreign Influence Reporting in Elections (FIRE) Act—recently introduced by Senator Mark Warner—although the requirements of the FIRE Act go beyond the recommendations in this report.

Moreover, some basic norms about engagement with foreigners should also be embraced proactively by all presidential candidates and their campaigns. For example, all candidates should avoid contact with foreigners to obtain compromising material on their opponents. In addition, they should not encourage foreign governments to steal property from their opponents and then promote the widespread dissemination of that illicit material.

6.4. Strengthen the norm of one government at a time.

Prior to Election Day, the president-elect and the incoming executive branch team should pledge to abstain from meeting with foreign government officials during their transition period, unless such a meeting has been approved and preferably attended by outgoing administration officials. This commitment would demonstrate high levels of transparency and accountability during a critical time of the electoral process, and would allow for appropriate transition planning while demonstrating that only one administration represents the United States at a time.

CHAPTER SEVEN

Establishing International Norms and Agreements to Prevent Election Interference

By Eileen Donahoe, Toomas Ilves, Chris Painter, Sergey Sanovich, Larry Diamond, Andrew Grotto, and Megan Metzger

The Problem

The United States is not the only country in the world to experience malicious, foreign interference during an election. Cyber interference in electoral processes and digital disinformation operations surrounding elections are an international phenomenon.[1] American policymakers rightly are focused on threats to election integrity in the United States in the run-up to the 2020 presidential vote, but these threats are part of a much larger, ongoing challenge to democracies everywhere. Because the problem is global, the American response must be both domestic *and* international. American government officials as well as the American private sector must recognize and underscore the global dimension of the threat and assume a leadership role in developing defenses against efforts to erode confidence in democracy. Reinforcement of international democratic governance norms in the digital context is vital. International law and other multilateral commitments already provide a substantial normative basis for action.[2]

One of the most important international norms of the post-World War II era is the right of the people of every country to freely choose their own government and determine their own future, enshrined in Article 21, Section 3 of the Universal Declaration of Human Rights (UDHR),[3] as well as in Articles 1 and 25 of the International Covenant on Civil and Political Rights (ICCPR).[4] Following these multilateral treaties, democratic norms and principles have subsequently been further codified in numerous regional and international agreements and declarations, including those of the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE), the European Union (EU), and the African Union (AU). Most recently, over 100 countries signed the Warsaw Declaration, a founding document of the Community of Democracies that defines global democratic norms and principles.

The world's democracies, including the United States, must reaffirm these principles and then translate and update them for the digital age. A range of stakeholders have undertaken important work to rearticulate and further develop norms for the cyber context. The U.S. government must now provide leadership and engage more systematically in developing and asserting these principles in the cyber realm.

Previous efforts in updating international norms for the digital age include the Tallinn Manual[5] and Tallinn Manual 2.0,[6] both of which were early efforts to support the application of existing international law to new cyber challenges, particularly relating to warfare. The Freedom Online Coalition was formed in 2011 and now includes 30 governments committed to reinforcing fundamental human rights principles in the digital realm.[7] In 2012, the United Nations Human Rights Council passed a consensus resolution affirming the applicability of fundamental human rights law in the digital space.[8] The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) also took steps to identify and promote international norms in the cyber realm. In a 2013 report, the UN GGE critically asserted that existing international law should be applied to cyber space and in its 2015 report, it articulated a list of eleven voluntary norms of state behavior. Unfortunately, the UN GGE process broke down in 2017 and was unable to reach a consensus. Though both a new GGE and an "Open Ended Working Group" on cyber issues will be launched in the UN this year, prospects for further substantive progress are uncertain. However, none of these prior efforts have dealt explicitly with issues around election interference.

Following the 2016 U.S. presidential election, a surge of individuals and groups[9] have joined the process of identifying norms to protect the integrity of elections, including the important work of articulating the distinction between legitimate efforts to promote democracy and illegitimate interference in the democratic processes of other countries.[10] Some stakeholders have argued that previous democracy promotion efforts of the U.S. and EU in other countries leave Americans and Europeans in a poor position to criticize the disruptive attempts of non-democratic countries.[11] We strongly disagree. There are important, identifiable differences between democracy promotion and unacceptable election interference. Democracy promotion is about ensuring that elections and other democratic processes reflect the will of the people; interference involves distorting the connection between the will of the people and representative government. Compelling analysis detailing these distinctions is beginning to emerge.[12]

This report has articulated dozens of concrete policy recommendations for enhancing the integrity and independence of the American electoral process in the run-up to the 2020 presidential vote. We believe that utilizing international norms more effectively can contribute both to the domestic American mission of protecting elections, while simultaneously building an international coalition dedicated to elections free of outside interference around the world.

Recommendations

7.1. Fortify U.S. and international commitment to human rights.

U.S. policymakers should begin by emphasizing the importance of existing international human rights law and norms. As noted in the UDHR and the ICCPR, as well as in numerous regional covenants and the Warsaw Declaration, these ratified agreements forbid states, groups, or persons from using any means to interfere with or subvert the ability of the people of a country

to choose their representatives and government through open and fair elections that are "free of fraud and intimidation."[13] Moreover, the President of the United States and senior leaders from both dominant political parties should forcefully denounce any attempt to subvert the sovereign right of the people to elect their representatives, through digital or any other means.

7.2. Strengthen international norms protecting election infrastructures.

The Group of Twenty (G20) and the UN GGE have both endorsed the U.S.-sponsored norm that "state[s] should not conduct or knowingly support ICT activity... that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[14] In 2016, the Secretary of Homeland Security formally designated electoral infrastructure as critical infrastructure.

The President of the United States and senior leaders from both dominant political parties should now emphasize the importance of existing norms on protecting critical infrastructure, which can be extended and reinforced in a digital context in several ways. As a starting point, all democracies should be encouraged to similarly acknowledge the obvious: that their election infrastructure, including the digital machinery of voter registration, vote casting, and other aspects of electoral administration, is critical infrastructure in accordance with their national critical infrastructure frameworks.

Furthermore, in line with the Transatlantic Commission on Election Integrity's pledge and the Global Commission on the Stability of Cyber Space's proposed norm protecting election systems, political leaders should assert that any effort to hack or otherwise infringe upon a country's electoral administrative and technical infrastructure—or any of its subnational electoral administrative jurisdictions—is illegitimate. This assertion would include any illicit effort to enter, view, or modify digital systems for voter registration, vote casting, or other aspects of electoral administration.

7.3. Create norms to deter the use of disinformation and hacked materials.

By definition, democracies already value and uphold strong norms against using violence and fraud to sway voters. As a form of fraud, disinformation campaigns thus violate fundamental democratic norms by producing, using, or spreading data and materials that were stolen, falsified, fabricated, illegally accessed, or doxed. Similarly, any effort to generate or knowingly distribute false information for the purposes of influencing an election should not be tolerated.

Consequently, political parties and candidates for office in democracies around the world should forge compacts agreeing to adhere to new norms about the production, use, or dissemination of such materials. For example, the Transatlantic Commission on Election Integrity has crafted a pledge and launched a process to seek widespread political recognition and support for such norms.[15] As discussed earlier in this report, both the Democratic and Republican parties, as well as their candidates and campaigns, should lead by example and pledge to strictly uphold these norms. Political parties in democracies around the world should similarly make a public commitment.

7.4. Lead international advocacy against foreign interference through disinformation. The United States should lead international advocacy in support of a norm against any organized fraudulent effort by a foreign entity—including by disguising the true source and nature of the intervention—to engage in, shape, stimulate, or inflame social media discourse for the purpose of distorting public opinion or political discourse, in particular during an election period.

7.5. Distinguish legitimate cross-border assistance from illicit or unlawful interventions. The distinction between legitimate forms of cross-border assistance to strengthen democratic electoral processes, including all aspects of electoral administration and the political environment for campaigning and voting, and illegitimate cross-border interventions to distort and subvert democratic electoral processes, must be clarified in the digital context and defended by democratic institutions. The UDHR recognizes that "the will of the people", as "expressed in periodic and genuine elections...with free voting procedures ...shall be the basis of the authority of government."[16] Because states have an obligation to respect the sovereignty of other countries and sovereignty resides in the people of the country, free and open elections are an indispensable means for determining "the will of the people." Democratic states have not only a right, but also an obligation to assist other peoples to express their will through free and fair elections.

The U.S. State Department, in parallel with similar institutions providing democratic assistance, should clearly articulate the following principles that differentiate legitimate from illegitimate engagement in this realm:

Democratic Intent: Any cross-border engagement with the electoral processes of another country should be done for the purpose of supporting the right to self-determination of the people of that country and to strengthen the integrity of electoral processes, so that universally accepted norms, as stipulated by the UDHR and by regional intergovernmental organizations, such as the OSCE, AU, and OAS, can be better realized.

Transparency: Cross-border engagement with the electoral processes of another country should be openly reported, with the exception of rare instances in which the personal safety of democratic actors is at risk. Furthermore, any involvement by a foreign government or non-state actor should be clearly disclosed by that entity. Engagement should be defined as any action that could affect the opinions or actions of citizens in favor of, or in opposition to, any candidate or party; the decision to participate or abstain from electoral participation; or the belief or confidence in elements of democratic governance.

Commitment to Trustworthy Information and Honest-Minded Discourse: State and non-state actors should refrain from propagating false or misleading information or producing fraudulent, inauthentic social media activity for the purpose of distorting or polarizing public opinion or

online political discourse, particularly during an election period. At the same time, state and non-state actors should strengthen the capacity of democratic media, parties, institutions, and organizations to detect, expose, and counter existing disinformation and manipulation of social media.

7.6. Hold congressional hearings about policies to support free and fair elections internationally.

The U.S. Congress should hold a series of hearings on U.S. government policies and programs to support free and fair elections internationally. Hearings would bring transparency to U.S. government efforts to promote democracy and help sharpen distinctions between appropriate and illegitimate behavior. Greater understanding of best practices to support free and fair elections internationally, including a discussion of efforts of other democracies beside the United States, could help to broaden more public support for these activities.

7.7. Promote cooperation among democracies focused on election protection.

Democratic countries should forge an international coalition to develop, support, and enforce universal norms of appropriate state behavior relating to non-interference in elections, as well as appropriate responses to illegitimate interference in elections. The coalition should establish one or more multilateral centers for sharing diagnostic information and intelligence, developing rapid situational analysis, and distributing this analysis in real time. The centers could be organized either as virtual organizations or brick and mortar institutions. Through the development of multilateral centers, democratic governments can strengthen both bilateral and multilateral forms of cooperation to identify and respond to digital threats to electoral integrity. They should also develop digital literacy initiatives for citizens and share effective strategies for building public resilience against disinformation. Moreover, government leaders from democratic states should meet at an annual summit to review disinformation trends and identify avenues for deepening existing methods of collaboration.

International cooperation is an essential element of the U.S. strategy to combat disinformation and establish new norms preventing electoral interference, as well as to reinforce the validity of previously articulated principles. States that respect the rule of law must cooperate[17] and collaborate[18] in addressing these issues.

7.8. Appoint a senior U.S. government representative on election interference.

The U.S. State Department should designate a senior-level official (ambassador-rank) to serve as the U.S. government lead for building coalitions with other countries to combat election interference and for developing and promoting overall norms on this topic. This official should work in coordination with American law enforcement, intelligence and other agencies to ensure adequate information sharing with foreign counterparts about disinformation campaigns and other malign interference with democratic processes. This official could be an existing official

with a compatible portfolio, such as the official charged with carrying out cyber policy, assuming that he or she is at least of ambassador rank.

7.9. Develop guidelines about platform cooperation with foreign governments.

The U.S. Department of Justice should prepare a legal opinion on the appropriate responses of digital and social media platforms if they are pressured by foreign governments to facilitate censorship, disseminate disinformation, or violate users' privacy. In addition, the U.S. Department of Justice should work with technology and human rights experts to establish community norms and guidelines for the acceptable level of cooperation between major social media platforms and foreign governments that engage in disinformation campaigns. The U.S. State Department should seek to synchronize such guidelines with the EU, other democratic countries, and relevant international bodies, and subsequently advocate for global recognition and enforcement of these guidelines to support platform integrity and to protect users' rights under international law.

CHAPTER EIGHT

Deterring Foreign Governments from Election Interference

By Herbert Lin, Chris Painter, and Andrew Grotto

The Problem

In deciding to interfere in the 2016 U.S. presidential election, Russian President Vladimir Putin calculated that the potential rewards were greater than potential costs. Given continued Russian interference, it is clear that American efforts to date have not changed his calculus. The U.S. government must impose timely, tailored, consistent and credible costs on Russia for aggression that both adequately penalize past conduct and serve as a deterrent for future interference. In so doing, the United States will help to deter other foreign governments from undertaking similar cyber actions both during the 2020 presidential election and more broadly.

The United States has taken some actions in response to Russian interference. For example, both the Obama and Trump administrations have imposed economic sanctions on Russian individuals and companies.[1] Secretary of State Mike Pompeo has asserted that the Trump administration has warned the Russian government about the negative consequences of future meddling, but the content of those threats has never been specified—making them impossible to assess—and their credibility is consistently undercut by contradictory messaging from the President.[2] There is news reporting about Cyber Command operations against Russian infrastructure, which we applaud in principle because they disrupt malicious activity and impose fleeting costs on Russia.[3] However, they are no substitute for a comprehensive, sustained campaign aimed at deterring interference from the Russian government or other foreign actors.

The lack of consistent and forceful U.S. action has had the opposite effect of deterrence, serving instead as a signal to Russia and other potential attackers that this is a relatively cost-free enterprise and encouraging more, not less, malicious activity.[4] The United States must do far more. Specifically, a deterrence strategy must be developed and executed to prevent foreign adversaries from intervening in American elections. To be effective and ultimately successful, a deterrence strategy must convince an adversary that the costs of taking a specific action will outweigh the benefits in a way that persuades that adversary to choose not to take that specific action.[5] Because deterrence concerns not only the objective facts of intentions, capabilities, and potential responses, but also the subjective perceptions of these facts by adversaries, the

consistency, credibility, and clarity of communication about one's intentions, capabilities, and potential responses are crucial. U.S. leaders must signal clearly the expected consequences in response to election interference and then commit credibly to taking that course of action before meddling occurs.

However, American leaders have thus far not signaled consistently, credibly, nor clearly about American intentions, capabilities, or potential responses to election interference. Most damagingly, President Trump has not even acknowledged the previous Russian attack, let alone denounce it, or outline clearly how he intends to deter future interventions. A recent report indicates that the President's Chief of Staff explicitly told Kirstjen Nielsen in the months before her resignation as Secretary of Homeland Security to refrain from discussing with the President preparations for new and different forms of interference by Russia in the 2020 election.[6]

Much of the theoretical discussion on deterrence originated during the Cold War, as researchers and policymakers sought to understand mechanisms for deterring adversaries from launching a nuclear attack. Bernard Brodie, Thomas Schelling, and Herman Kahn were among the most prominent theorists who articulated theories that rational adversaries can be deterred if they assess that the costs of a course of action exceed the benefits.[7] A critical element of these theories is that the adversary must believe in the credibility of claims about those costs. These ideas underpinned Cold War nuclear doctrine and remain more-or-less implicit in much of American nuclear posture up to the present, despite some valid criticism of their strength and legitimacy in light of newer findings about decision-making in cognitive psychology.[8] Deterrence theory also shapes Russian nuclear doctrine considerably. However, less well understood is the extent to which a variety of direct actions short of war—be they clandestine, covert, cyber, cyber-enabled, psychological, or propaganda—taken by one nuclear power against another might be effectively deterred.

The United States has acknowledged the necessity of deterrence in cyberspace and taken several related actions. In the 2011 International Strategy for Cyberspace, the United States stated that it would use the full range of tools, including diplomatic, economic (including sanctions), law enforcement, cyber, and even kinetic military actions to respond to appropriate cyberattacks.[9] President Obama signed an executive order authorizing the use of economic sanctions against actors assessed to have participated in malicious cyber actions against critical infrastructure and other targets, while the U.S. Congress and the Trump administration have issued sanctions regimes to deal with election interference. The U.S. State Department's May 2018 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats" call for a new policy "for when the United States will impose consequences", a menu of "swift, costly, and transparent" consequences, and better policy planning and international partnerships to impose these consequences.[10] If effectively implemented, these steps could be successful and further strengthened by consistent, high-level messaging regarding the explicit threat of cost imposition asymmetrically and across domains. To succeed, however, these threats must be credible.

As noted earlier, U.S. Cyber Command reportedly conducted operations aimed at knocking the Internet Research Agency (IRA) offline on the day of the 2018 midterm elections, though the U.S. government has not publicly acknowledged this action.[11] Although this particular operation, if accurately reported as being focused on disrupting operations during Election Day, was a good start, it nevertheless was too little and too late. As discussed in other chapters, the IRA engages in medium- to long-term propaganda efforts that weaponize social media to undermine public trust in Western institutions, amplify societal polarization, and destabilize perception vis-à-vis truth and factual evidence. If the IRA were operating in the 2018 U.S. midterm elections, as it did during the 2016 U.S. presidential elections, significant damage would have already been inflicted prior to Election Day.[12] Rather than conducting similarly limited operations, the United States needs to impose costs in a strategic way, acting together, when possible, with allies and partners.

Moreover, U.S. government activity in cyberspace often appears to be too quiet to deliver a deterrent message. There clearly is a place for concealed activity with regard to disruption–especially if such disruption is to sow confusion in the adversaries' ranks. But if the purpose is, even in part, deterrence, then the United States should be more willing to claim responsibility, even if it is after the fact. If the United States communicates either privately or publicly to the adversary that it is taking action, it demonstrates both a willingness and capability to act (helping to deter future conduct) and opens up potential channels of de-escalation through clear military, intelligence, and diplomatic communications channels.

Recommendations

8.1. Recalibrate risk tolerances for actions in cyberspace.

To be more successful in deterring adversary behavior, the United States must begin by increasing its willingness to accept greater risk of adversary retaliation, including retaliation in the cyber domain. Today, U.S. opponents are counting on American aversion to cyber risk in order to deter U.S. responses.[13] When risk-aversion dominates policymaking, the choice to take no action is privileged. What is necessary instead is a long-term strategy that frames the costs of inaction in terms of both the present and future malicious adversary behavior that inaction enables.

8.2. Signal a clear and credible commitment to respond to election interference.

From the top down, and including most importantly from the President, the U.S. government must demonstrate a clear, credible, and consistent commitment in response to future attempts at election interference.[14] U.S. leaders should detail specifically what costs will be imposed on attacking adversaries and, when election interference occurs, actually impose those costs. The worst of all outcomes is drawing red lines without delivering on them. Clear, credible, and consistent commitments to respond and follow-through are crucial to deterrence; in their absence, an adversary is more likely to gamble and believe that the United States is bluffing.

Among other conditions, mandatory response regimes, similar but not necessarily identical to the one contemplated in the DETER Act calling for mandatory sanctions to be imposed upon a determination by the Director of National Intelligence that a foreign power had interfered in a U.S. federal election, should be enacted and implemented.[15]

8.3. Maintain a visible position of U.S. capabilities, intentions, and responses.
Deterrent responses from the United States should not be entirely concealed from the adversary, but this requirement does not imply necessarily that the American response must be made public. Specifically, if the intent of a response to penalize meddling or deter future meddling, the adversary must understand that the United States is responding (or has responded) to meddling and that penalties will continue unless the adversary's behavior changes. It should also be signaled or communicated to the adversary that penalties will cease when its behavior changes. Clear signaling can be conveyed publicly or privately, during presidential summits, calls, and written communications or private meetings between diplomats or intelligence officers. Actions can also send signals, though care must be taken to ensure that the adversary actually gets the message. The mode of signaling should be calibrated to maximize impact while minimizing retaliatory and other risks—private signaling might allay the domestic political need for an adversary leader to respond to a perceived threat from the United States and serve as a means of de-escalation if needed. The U.S. State Department's proposed new policy on transparent deterrence responses should be fleshed out and released swiftly,[16] as should incorporate asymmetric and cross-domain responses recommended below.

8.4. Enact country-specific and timely responses that impose real, effective costs.
American policymakers should take appropriate deterrence responses, which are not only country-specific and timely, but also impose real costs on adversaries. Cost imposition need not be in the same domain—U.S. decisionmakers should consider responding in a domain unrelated to the one in which the original incident occurred. In addition to more traditional diplomatic sanctions, law enforcement, and cyber tools, response options can span the full range of dealings between the United States and the country at issue and could include anything from trade to immigration—as long as it places at risk something the adversary wants until their behavior changes.[17]

Examples of responsive actions that could be considered, subject to the caveats below, include more targeted economic sanctions on the adversary, restrictions on travel to the United States, or targeted economic sanctions on the adversary's agents and close friends.[18] Various kinds of covert action could also be considered, including targeted action against the financial holdings of the key individuals responsible for meddling. With respect to the Russian government, publication of true information about corruption or illicit financial dealings is another instrument of deterrence to maintain in the American arsenal.

U.S. decisionmakers must also keep in mind that a meaningful response from the United States is likely to provoke a counterreaction, and therefore insights of the intelligence community regarding such counterreactions should be sought and taken into account in determining the wisdom of taking such actions in the first place. In other words, concerns about the scope and nature of a likely counterreaction should not deter the United States from responding (see recommendation 1), but the United States should proceed knowing to the extent possible the risks from any given U.S. response.

Furthermore, U.S. actions to impose costs for bad behavior must be accompanied by credible promises to cease cost imposition activities once bad behavior has terminated. Otherwise, the adversary will have no particular incentive to stop its own aggressive behavior.

8.5. Promote collective engagement with international partners.

Deterrence is more effective and impactful when done collectively rather than acting alone. Perceptions of credibility and commitment to take substantial and significant actions in response to election interference are strengthened when they come from a coalition of countries and multilateral organizations working in solidarity. Building a coalition of countries to take collective action is a stated goal of the State Department's deterrence initiative and should be fully resourced and supported. Although there has been some success in joint attribution efforts with respect to Russian and North Korean malicious cyber activity, the practice of "naming and shaming" those countries is unlikely to change their malign behavior absent cost imposition. Achieving collective cost imposition, however, will require more than diplomacy and coalition building. Among other things, information sharing with partners will need to be improved to enable those partners to act and get needed political-level buy-in for taking action. Partners will also need to expand their ability to impose substantial costs.[19] In addition, as discussed in greater detail in Chapter Seven, the international community must come together to establish norms against electoral interference. The next step would be to transparently agree on cost-imposing responses to those countries who violate these norms.

8.6. Conduct a continuous strategic disruption campaign against adversaries that seek to interfere with U.S. elections.

At its most effective level, election interference is not so much an event as an ongoing adversary activity. Accordingly, the United States must conduct its counter-interference efforts as a strategic campaign rather than as a one-time response. Strategic campaigns are, of course, defined by consistent effort over time and coherent strategy, and should be directed specifically against the offending actors (i.e., those individuals and organizations most closely involved with the interference activities). Note, however, that in conducting such a campaign, the United States should be aware that conducting cyber operations unilaterally in non-adversary space can place at risk partnerships with those countries that might otherwise be willing to take future collective action.

8.7. Pursue common interests in cyberspace where possible.

As highlighted in the beginning of this chapter, the United States has failed to impose costs on Russia adequate to deter meddling in U.S. elections, and so the previous recommendations propose various measures to increase costs to Russia as a consequence of continuing interference. Such actions also will deter other foreign actors. Nevertheless, the necessity of taking such measures should not blind the United States to the reality that the United States and Russia must have communication channels and do have common interests that are worth exploring despite the adversarial relationship between the two nations. Eventually, not unlike nuclear arms control negotiations during the Cold War, we must be able to credibly deter and to establish some rules of the road for preventing catastrophic outcomes at the same time. First, the United States should ensure that there are adequate formal and informal communication channels—military, intelligence, and diplomatic—to allow for appropriate signaling and de-escalation as the deterrence strategy is being implemented. Such channels also can help to avoid misperception or misattribution in the event of a third-party cyber operation seeking to provoke further conflict or escalate tensions between the two nations. For example, working and technical level talks to make sure the U.S.-Russia cyber hotline is operational and tested would ensure that this communication channel is available when needed.

In addition, the United States, when appropriate, should support the establishment of working groups between the two nations and encourage unofficial Track 2 dialogues to explore the shape and nature of carefully scoped common interests. For example, both nations share commitments to fight child pornography and human trafficking, activities that rely in large measure on cyber-enabled communications. Neither nation wants the other nation to suffer cyberattacks that increase the likelihood of accidental nuclear conflict. Discussions about such topics (or others—these are merely illustrative) could lead to mutual actions that serve the interests of both the United States and Russia, and as importantly could help to establish and sustain channels of communication that would prove valuable in the future.

Of course, in commissioning any formal government discussions, the United States must be careful not to inadvertently signal to Russia or the rest of the world that it has simply forgiven Russia's past and continuing election meddling and other malicious cyber conduct. Russia has long sought to re-establish the high-level, political cyber dialogue (that was suspended, like other such dialogues, following Russia's incursions into Ukraine), in part, for this very purpose. Unless and until there are significant commitments by Russia and substantial changes in Russia's actions, any high-level cyber dialogue is at best premature and at worst simply a public relations coup that would be seen as rewarding them for their disruptive conduct. And even if such a dialogue on cyber issues starts again in the future, the United States must continue to deter Russia's belligerent behavior in other domains, including first and foremost in Europe in general and Ukraine in particular.[20] During the Cold War, U.S. administrations managed to engage their

Soviet counterparts on nuclear arms control issues, while simultaneously containing the Soviet Union on other fronts. Regarding cyber issues and other confrontational areas of the current U.S.-Russian agenda, we can pursue a similarly sophisticated, dual track strategy of engagement and containment again.

PREFACE

1 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice,* March 2019, Page 1.

2 Thomas H. Kean et al., "The 9/11 Commission Report," https://www.9-11commission.gov/report.

3 Bart Jansen, Tom Vanden Brook, Kevin Johnson, and William Cummings, "Mueller's investigation is done. Here are the 34 people he indicted along the way," *USA Today,* March 25, 2019, https://www.usatoday.com/story/news/politics/2019/03/25/muellers-russia-report-special-counsel-indictments-charges/3266050002/.

4 Sonam Sheth and Pat Ralph, "The House Intel Committee report on its controversial Russia investigation is out — here are the big points," *Business Insider,* April 27, 2018, https://www.businessinsider.com/house-intel-committee-report-russia-investigation-2018-4.

5 Julian E. Barnes and Adam Goldman, "F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations," *The New York Times,* April 26, 2019, https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

6 The authors acknowledge that this report draws from and builds on research and insights produced by the following studies: "A Guide to Cyber Attribution," Office of the Director of National Intelligence, September 14, 2018; "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation," European Commission, 2018; "A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the 'See it, Sense it, Share it, Use it' approach to thinking about Cyber Intelligence," Office of the Director of National Intelligence, October 2018; Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data & Society Research Institute; Ann M. Ravel, Samuel C. Woolley, and Hamsini Sridharan, "Principles and Policies to Counter Deceptive Digital Policies," MapLight, February 2019; Ben Judah and Nate Sibley, "Countering Russian Kleptocracy," Hudson Institute, April 2018, https://s3.amazonaws.com/media.hudson.org/files/publications/CounteringRussianKleptocracy.pdf; "Building Blocks of Cyber Intelligence," Office of the Director of National Intelligence; Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, 2016, https://www.rand.org/pubs/perspectives/PE198.html; David P. Fidler, "The U.S. Election Hacks, Cybersecurity, and International Law," Indiana University, Maurer School of Law, 2017; Dipayan Ghost and Ben Scott, "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet," Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, September 2018; Dipayan Ghost and Ben Scott, "#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet," Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, January 2018; "Disinformation and 'fake news': Final Report," House of Commons: Digital, Culture, Media and Sport Committee, February 18, 2019; Gordon Ramsay and Sam Robertshaw, "Weaponising news: RT, Sputnik and targeted disinformation," King's College London, the Policy Institute, Centre for the Study of Media, Communication & Power; John W. Kelly, "Briefing for the United States Senate Select Committee on Intelligence," Graphika, August 1, 2018; Margaret Roberts, "Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy," May 4, 2017; "Draft Charter: An Oversight Board for Content Decisions," Facebook; "Midterm Assessment: the Trump Administration's Foreign and National Security Policies," Foundation for Defense of Democracies, edited by John Hannah and David Adesnik, January 2019; Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 2018; "Examining Foreign Interference in U.S. Elections," Campaign Legal Center, January 2018; "Fighting Fake News: Workshop Report," The Information Society Project, the Floyd Abrams Institute for Freedom of Expression; "Forbidden Feeds: Government Controls on Social Media in China," PEN America, March 13, 2018; Geir Haugen, "Manipulation and Deception with Social Bots: Strategies and Indicators for Minimizing Impact," Norwegian University of Science and Technology, May 2017; Greg Miller, The Apprentice: Trump, Russia and the Subversion of American Democracy (New York: HarperCollins, 2018); Kathleen Hall Jamieson, How Russian Hackers and Trolls Helped Elect a President (Oxford: Oxford University Press, 2018); "International Security and Estonia: 2018," Estonian Foreign Intelligence Service; Jamie Fly and Laura Rosenberger, "The Mueller Report Shows Politicians Must Unite to Fight Election Interference," German Marshall Fund, April 22, 2019, http://www.gmfus.org/commentary/mueller-report-shows-politicians-must-unite-fight-election-interference; Jamie Fly, Laura Rosenberger, and David Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies," German Marshall Fund, June 26, 2018, http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies; Joshua A. Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, "Social

Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature," William and Flora Hewlett Foundation, March 2018; Laura Galante and Shaun Ee, "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Enabled Incidents," Atlantic Council, the Brent Scowcroft Center for Strategy and Security, September 2018; Laura Rosenberger, "Statement of Laura Rosenberger, Alliance for Securing Democracy, the German Marshall Fund of the United States, Before the United States Senate Select Committee on Intelligence Concerning 'Foreign Influence Operations and their use of Social Media Platforms'", United States Senate Select Committee on Intelligence, August 1, 2018; "'Make Germany Great Again': Kremlin, Alt-Right and International Influences in the 2017 German Elections," London School of Economics, Institute of Global Affairs, Institute for Strategic Dialogue; Malcolm Nance, The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West (New York: Hachette, 2018); Michael Isikoff and David Corn, Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump (New York: Twelver 2018); Michael McFaul, "Testimony of Ambassador Michael McFaul, Putin's Playbook: the Kremlin's Use of Oligarchs, Money and Intelligence in 2016 and Beyond," U.S. House Permanent Select Committee on Intelligence, March 28, 2019; "Online and On All Fronts: Russia's Assault on Freedom of Expression," Human Rights Watch, 2017; Paul M. Barrett, "Tackling Domestic Disinformation: What the Social Media Companies Need to Do," NYU Stern, Center for Business and Human Rights, March 2019; Paul M. Barrett, Tara Wadhwa, and Dorothé Baumann-Pauly, "Combating Russian Disinformation: The Case for Stepping Up the Fight Online," NYU Stern, Center for Business and Human Rights, July 2018; Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," University of Oxford, Computational Propaganda Research Project; Philip N. Howard, "Testimony of Philip N. Howard, Oxford University, 'Foreign Influence on Social Media Platforms: Perspectives from Third-Party Social Media Experts,'" United States Senate Select Committee on Intelligence, August 1, 2018; Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," New Knowledge; Richard Fletcher, Alessio Cornia, Lucas Graves, and Rasmus Kleis Nielsen, "Measuring the reach of 'fake news' and online disinformation in Europe," University of Oxford, Reuters Institute for the Study of Journalism, February 2018; "Robotrolling: Issue 1," NATO Strategic Communications Centre of Excellence, 2017; "Robotrolling: Issue 2," NATO Strategic Communications Centre of Excellence, 2017; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," University of Oxford, Computational Propaganda Research Project; Seth Abramson, Proof of Collusion: How Trump Betrayed America (New York: Simon and Shuster, 2018); "SSCI Research Summary December 1, 2018: An assessment of the Internet Research Agency's U.S.-directed activities in 2015-2017 based on platform-provided data," New Knowledge; Timothy Garton Ash, Robert Gorwa, and Danaë Metaxa, "GLASTNOST! Nine ways Facebook can make itself a better forum for free speech and democracy: An Oxford-Stanford Report," University of Oxford, Reuters Institute for the Study of Journalism; Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," Rand Corporation; Todd C. Helmus, "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe: Testimony before the Senate Select Committee on Intelligence," Rand Corporation, August 1, 2018; Whitney Phillips, "The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online," Data & Society Research Institute; "Who Said What? The Security Challenges of Modern Disinformation: Highlights from the Workshop," Canadian Security Intelligence Service, February 2018.

7 In addition to the authors of the chapters, I am deeply grateful to Bronte Kass and Kimberly Renk for their editorial and research assistance in completing this report.

SUMMARY OF RECOMMENDATIONS

1 Authors of individual chapters clearly support the recommendations in their chapters but do not necessarily endorse the recommendations in other chapters.

CHAPTER ONE

1 Additional thanks to Anya Shkurko and Anna Manafova for their research contributions to this chapter.

2 For a deeper elaboration of 'Putinism', see Michael McFaul, "Putinism and the 2016 U.S. Presidential Election," (Working Paper, February 2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/putinisn2016election-3-10-19_1.pdf.

3 "Speech and the Following Discussion at the Munich Conference on Security Policy," *The Kremlin,* February 10, 2007, http://en.kremlin.ru/events/president/transcripts/24034.

4 For elaboration, see: ВРЕМЕННАЯ КОМИССИЯ СОВЕТА ФЕДЕРАЦИИ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА И ПРЕДОТВРАЩЕНИЮ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА РОССИЙСКОЙ ФЕДЕРАЦИИ: СПЕЦИАЛЬНЫЙ ДОКЛАД ПО ИТОГАМ ПРЕЗИДЕНТСКИХ ВЫБОРОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ (2018 г.) С ТОЧКИ ЗРЕНИЯ ПОКУШЕНИЙ НА РОССИЙСКИЙ ЭЛЕКТОРАЛЬНЫЙ СУВЕРЕНИТЕТ, http://council.gov.ru/media/files/2uQuCAAwoWu0B8tiDeDExn5x9CtBkTDV.pdf. In this final report, issued by "The interim commission of the council of federation for the protection of state sovereignty and prevention of the interference in the internal affairs of the Russian Federation", the authors claim that in addition to interfering with the affairs of other sovereign states, the United States has been meddling in Russian affairs since the dissolution of the USSR through undermining the Russian government and dividing Russian society, whether acting directly in the country or indirectly through third countries or organizations. The authors of the report claim that Americans are funding Russian civil society organizations, think tanks, non-governmental organizations, journalists, and even individual activists to undermine Russian sovereignty from within. Simultaneously, they assert that in partnership with NATO member countries, the United States actively participated in destabilizing the situation in the Middle East and Northern Africa during the "Arab Spring", just around the time of Russian elections of 2011-12.

5 Gillian Edevane, "NRA Admits Accepting Money from 12 Russia-Linked Donors," *Newsweek,* April 11, 2018, https://www.newsweek.com/nra-admits-accepting-money-23-russia-linked-donors-882310.

6 Paul Sonne, "A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *The Washington Post,* December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a504-22_story.html?utm_term=.d38f1372ea01.

7 Edward Delman, "When is a TV Channel a Foreign Agent?" *The Atlantic,* April 22, 2015, https://www.theatlantic.com/international/archive/2015/04/rt-lobbyist-russia-putin-media/390621/. For a deeper analysis of RT efforts on YouTube, see Robert Orttung and Elizabeth Nelson, "Russia Today's strategy and effectiveness on YouTube," *Post-Soviet Affairs* 35, no. 2 (2019): 77-92.

8 For background, see Sergey Sanovich, "Russia: The Origins of Digital Misinformation," in *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media,* ed. Samuel Wooley and Philip Howard (Oxford: Oxford University Press, 2019), 21-40.

9 Neil MacFarquhar, "Outrage Grows as Russia Grants Passports in Ukraine's Breakaway Regions," *The New York Times,* April 25, 2019, https://www.nytimes.com/2019/04/25/world/europe/russia-citizenship-ukraine.html.

10 For details, see Michael McFaul, *From Cold War to Hot Peace: An American Ambassador in Putin's Russia* (Houghton Mifflin Harcourt, May 2018), 239-63.

11 Blair Miller, "Trump election fraud commission wants personal information from Colorado, US voter rolls," *The Denver Channel,* June 29, 2017, https://www.thedenverchannel.com/decodedc/for-trump-supporters-election-fraud-is-a-real-fear.

12 Tyler Pager, "Trump to Look at Recognizing Crimea as Russian Territory, Lifting Sanctions," *Politico,* July 27, 2016, http://www.politico.com/story/2016/07/trump-crimea-sanctions-russia-226292.

13 Carol Morello and Adam Taylor, "Trump Says U.S. Won't Rush to Defend NATO Countries if They Don't Spend More on Military," *The Washington Post,* July 21, 2016, https://www.washingtonpost.com/world/national-security/trump-says-us-wont-rush-to-defend-nato-countries-if-they-dont-spend-more-on-military/2016/07/21/76c48430-4f51-11e6-a7d8-13d06b37f256_story.html?tid=a_inl&utm_term=.c864abc4ab0c. Candidate Trump actually argued inaccurately that NATO allies were not paying enough to the United States. NATO does not operate that way. For elaboration, see Michael McFaul, "Mr. Trump, NATO Is an Alliance, Not a Protection Racket," *The Washington Post,* July 25, 2017, https://www.washingtonpost.com/opinions/global-opinions/mr-trump-nato-is-an-alliance-not-a-protection-racket/2016/07/25/03ca2712-527d-11e6-88eb-7dda4e2f2aec_story.html?utm_term=.4f2db182f676.

14 Alex Griswold, "Trump Defends Putin's Murder of Journalists: 'Our country Does Plenty of Killing Also,'" *Mediaite,* December 18, 2015, https://www.mediaite.com/tv/donald-trump-defends-putins-murder-of-journalists-our-country-does-plenty-of-killing-also/.

15 Abby Philip, "O'Reilly Told Trump That Putin Is a Killer. Trump's Reply: 'You Think Our Country Is So Innocent?'" *The Washington Post,* February 4, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/02/04/oreilly-told-trump-that-putin-is-a-killer-trumps-reply-you-think-our-countrys-so-innocent/?utm_term=.5d54f7ad3b79.

16 "Presidential Candidate Donald Trump Primary Night Speech," *C-SPAN,* April 26, 2016, https://www.c-span.org/video/?408719-1/donald-trump-primary-night-speech&start=1889&transcriptQuery=putin.

17 Jeremy Diamond, "Timeline: Donald Trump's praise for Vladimir Putin," *CNN,* July 29, 2016, http://www.cnn.com/2016/07/28/politics/donald-trump-vladimir-putin-quotes/index.html and Andrew Kaczynski, "80 Times Trump Talked about Putin," *CNN,* March 2017, http://www.cnn.com/interactive/2017/03/politics/trump-putin-russia-timeline/.

18 "Donald Trump Campaign Rally in Hilton Head, South Carolina," *C-SPAN,* December 30, 2015, https://www.c-span.org/video/?402610-1/donald-trump-campaign-rally-hilton-head-south-carolina&transcriptQuery=putin&start=787.

19 "Donald Trump Campaign Rally in Vandalia, Ohio," *C-SPAN,* March 12, 2016, https://www.c-span.org/video/?406393-1/donald-trump-campaign-rally-vandalia-ohio&transcriptQuery=putin&start=1907.

20 Reena Flores, "Donald Trump gives Russia's Putin an 'A' in leadership," *CBS News,* September 30, 2015, https://www.cbsnews.com/news/donald-trump-gives-russias-putin-an-a-in-leadership/.

21 On the differences between President Trump and his administration regarding Russia policy, see Michael McFaul, "Sorry, but Trump is not 'tough on Russia'," *The Washington Post,* January 19, 2019, https://www.washingtonpost.com/opinions/2019/01/16/sorry-trump-is-not-tough-russia/?utm_term=.fb100c094e50.

22 "Background to 'Assessing Russian Activities and Intentions on Recent US Elections': The Analytic Process and Cyber Incident Attribution," *Office of the Director of National Intelligence,* January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

23 "Remarks by President Trump and President Putin of the Russian Federation in Joint Press Conference," *The White House,* issued on July 16, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/

24 Hillary Clinton, *What Happened* (Simon & Schuster, 2017), 327.

25 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice,* March 2019, 1 ("Mueller Report").

26 Ibid.

27 Ibid., 9.

28 The counterintelligence component of the Special Counsel investigation has not been published and is most likely ongoing.

29 Mueller Report, 4. The Special Counsel Office charged 12 GRU officers for crimes arising from the hacking of these computers, principally with conspiring to commit computer intrusions, in violation of 18 U.S.C. §§1030 and 371. See Volume I, Section V.B, infra; Indictment, United States v. Netyksho, No. I :18-cr-215 (D.D.C. July 13, 2018), Doc. 1 ("Netyksho Indictment").

30 Netyksho Indictment, r 1.

31 Separate from the Special Counsel Office's indictment of GRU officers, in October 2018 a grand jury sitting in the Western District of Pennsylvania returned an indictment charging certain members of Unit 26165 with hacking the U.S. Anti-Doping Agency, the World Anti-Doping Agency, and other international sport associations. United States v. Aleksei Sergeyevich Morenets, No.18-263 (W.D. Pa.).

32 Netyksho Indictment, paragraph 9.

33 Mueller Report, 37.

34 Ibid., 38.

35 Ibid.

36 Ibid., 41.

37 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike Blog,* June 14, 2016. CrowdStrike updated its post after the June 15, 2016 post by Guccifer 2.0 claiming responsibility for the intrusion.

38 Releases of documents on the Guccifer 2.0 blog occurred on June 15, 2016; June 20, 2016; June 21, 2016; July 6, 2016; July 14, 2016; August 12, 2016; August 15, 2016; August 21, 2016; August 31, 2016; September 15, 2016; September 23, 2016; October 4, 2016; and October 18, 2016.

39 Mueller Report, 43.

40 Ibid., 44.

41 James Ball, "Julian Assange could face arrest in Australia over unredacted cables," *The Guardian,* September 2, 2011, https://www.theguardian.com/media/2011/sep/02/julian-assange-arrest-australia-wikileaks.

42 Mueller Report, 48.

43 7/6/16 Twitter DMs, @WikiLeaks & @guccifer_2.

44 Mueller Report, 51.

45 Ibid., 53.

46 Ibid., 59.

47 At the time, the link took users to a WikiLeaks archive of stolen Clinton campaign documents.

48 10/12/16 Twitter DM, @WikiLeaks to @DonaldJTrumpJr.

49 @DonaldJTrumpJr 10/14/16 (6:34 a.m.) Tweet.

50 Mueller Report, 62. Flynn 4/25/18 302, at 5-6; Flynn 5/1/18 302, at 1-3; Flynn 5/1/18 302, at 1-3.

51 "Donald Trump on Russian & Missing Hillary Clinton Emails," *C-SPAN,* Posted 7/27/16, available at https://www.youtube.com/watch?v=3kxG8uJUsWU (starting at 0:41).

52 Mueller Report, 36, 58.

53 Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2019).

54 Mueller Report, 4.

55 Colin Stretch, *Social Media influence in the 2016 U.S. election, hearing before the senate select committee on intelligence,* 115th Congr. 13 (11/1/17).

56 Ibid.

57 Eli Rosenberg, "Twitter to Tell 677,000 Users they Were Had by the Russians. Some Signs Show the Problem Continues," *The Washington Post,* January 19, 2019; Twitter, "Update on Twitter's Review of the 2016 US Election," updated January 31, 2018. Twitter also reported identifying 50,258 automated accounts connected to the Russian government, which tweeted over a million times in the ten weeks before the election.

58 Gerrit De Vynck and Selina Wang, "Russian Bots Retweeted Trump's Twitter 470,000 Times," *Bloomberg,* updated January 29, 2018, https://www.bloomberg.com/news/articles/2018-01-26/twitter-says-russian-linked-bots-retweeted-trump-470-000-times.

59 Politico Staff, "The social media ads Russia wanted Americans to see," *Politico,* November 1, 2017, https://www.politico.com/story/2017/11/01/social-media-ads-russia-wanted-americans-to-see-244423.

60 Mueller Report, 24-25.

61 4/19/16 Facebook Advertisement ID 6045151094235.

62 Mueller Report, 26.

63 Instagram ID 2228012168 (Stand For Freedom) 11/3/15 Post ("Good evening buds! Well I am planning to organize a confederate rally[...] in Houston on the 14 of November and I want more people to attend.").

64 Mueller Report, 31-32.

65 Ibid., 19-20.

66 Ibid.,16.

67 "Internet Agency Indictment," *U.S. Department of Justice*, filed February 16, 2018. https://www.justice.gov/file/1035477/download,12(b); see also 5/26/16 Facebook Messages, ID 1479936895656747 (United Muslims of America).

68 "Internet Agency Indictment".

69 Mueller Report, 21.

70 Ibid., 5.

71 For example, on August 18, 2015, on behalf of the editor-in-chief of the internet newspaper Vzglyad, Georgi Asatryan emailed campaign press secretary Hope Hicks asking for a phone or in-person candidate interview. 8/18/15 Email, Asatryan to Hicks. One day earlier, the publication's founder (and former Russian parliamentarian) Konstantin Rykov had registered two Russian websites-Trump2016.ru and DonaldTrump2016.ru. No interview took place.

72 Mueller Report, 71. 11/3/15 Email, Sater to Cohen (12:14p.m.).

73 Mueller Report, 5.

74 Ibid., 5-6.

75 Ibid., 6.

76 DJTJR00446 (6/3/16 Email, Trump Jr. to Goldstone); @DonaldJTrumpJr 07/11/17 (11:00) Tweet; RG000061 (6/3/16 Email, Trump Jr. to Goldstone).

77 Natasha Bertrand, "Putin's Big Tell?" *The Atlantic*, July 18, 2018, https://www.theatlantic.com/politics/archive/2018/07/putins-big-tell/565460/.

78 Mueller Report, 110.

79 Approximately one year later, the June 9 meeting became public and immediately provocative with regards to its implications. In a July 9, 2017 text message to Emin Agalarov, Goldstone wrote, "I made sure I kept you and your father out of [t]his story," and "[i]f contacted I can do a dance and keep you out of it," adding, "FBI now investigating," and "I hope this favor was worth for your dad-it could blow up." See Mueller Report, 121.

80 Ibid., 6-7.

81 As noted in Volume I, Section III. D.I.b, supra, Gates pleaded guilty to two criminal charges in the District of Columbia, including making a false statement to the FBI, pursuant to a plea agreement. He has provided information and in-court testimony that the Office has deemed to be reliable. See also Transcript at 16, United States v. Paul J Manafort, Jr., l:17-cr-201 (D.D.C. Feb. 13, 2019), Doc. 514 ("Manafort 2/13/19 Transcript") (court's explanation of reasons to credit Oates's statements in one instance).

82 Mueller Report, 129.

83 Ibid., 140.

84 Ibid., 9.

85 "Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Russian Intelligence hearing titled 'Russian Interference in the 2016 U.S. Elections,'" *U.S. Department of Homeland Security*, June 21, 2017, https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

86 Pam Fessler, "Mueller Report Raises New Questions about Russia's Hacking Targets in 2016," *NPR,* April 19, 2019, https://www.npr.org/2019/04/19/714890832/mueller-report-raises-new-questions-about-russias-hacking-targets-in-2016.

87 Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions," *NPR,* August 10, 2017, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

88 Mueller Report, 50.

89 Ibid.

90 Ibid., 51.

91 For an assessment, see chapters ten and eleven in Morris Fiorina, *Unstable Majorities: Polarization, Party Sorting & Political Stalemate* (Stanford: Hoover Institution Press, 2017).

92 For a careful treatment of this difficult social science question, see Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2019).

93 Cooperative Congressional Election Study, as quoted in Danielle Kurtzleben, "Here's How Many Bernie Sanders Supporters Ultimately Voted for Trump," *NPR,* August 24, 2017, http://www.npr.org/2017/08/24/545812242/1-in-10-sanders-primary-voters-ended-up-supporting-trump-survey-finds?utm_source=twitter.com&utm_medium=social&utm_campaign=politics&utm_term=nprnews&utm_content=20170824.

94 Jamieson, *Cyber-War,* Appendix One.

95 "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project,* https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

96 According to the National Urban League's 2019 State of Black America report. the use of race as a weapon to divide Americans and dissuade African-American populations from voting has been largely overlooked in the public discussion of Russian interference. See "State of Black America," *National Urban League,* 2019, http://soba.iamempowered.com/2019-report.

97 "The Tactics and Tropes of the Internet Research Agency," *New Knowledge,* December 17, 2018, https://www.newknowledge.com/disinforeport.

98 Mirren Gidda, "Third Party Votes Could Have Cost Hillary Clinton the Presidency," *Newsweek,* November 9, 2016, http://www.newsweek.com/susan-sarandon-third-party-candidates-jill-stein-gary-johnson-hillary-clinton-519032.

99 Bruce Schneier, "Defending Democracies Against Information Attacks," *Schneier on Security,* April 30, 2019, https://www.schneier.com/blog/archives/2019/04/defending_democ.html.

100 Todd Ruger, "FBI director wants to 'up our game' on election interference," *Roll Call,* May 7, 2019, https://www.rollcall.com/news/congress/fbi-director-wants-game-election-interference.

CHAPTER TWO

1 "Help America Vote Act," *U.S. Election Assistance Commission,* accessed April 16, 2019, https://www.eac.gov/about/help-america-vote-act/.

2 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice,* March 2019, 49-51 ("Mueller Report").

3 Ibid., 51.

4 Julian E. Barnes and Adam Goldman, "F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations," *The New York Times,* April 26, 2019, https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html.

5 National Research Council, "Letter Report on Electronic Voting," *The National Academies Press,* 2006, https://www.nap.edu/catalog/11704/letter-report-on-electronic-voting.

6 The 2016 election was arguably not a close election, as Donald Trump lost the popular vote by 2.8 million votes, a margin of 2% of the total number of votes cast. But victories in individual states determine the electoral vote count, and in three key states, Trump won the popular vote by about 107,000 people, or a margin of 0.09 percent of all votes cast in this election, leading to his victory in the Electoral College. By any measure, a winning margin of 0.09 percent is very close indeed. See Tim Meko, Denise Lu, and Lazaro Gamio, "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016, https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

7 National Research Council, "Cybersecurity Today and Tomorrow: Pay Now or Pay Later," (Washington, DC: National Academy Press, 2002).

8 More precisely, concealing the internal operation of a system does provide a layer of protection for a system. But because concealment does not actually fix vulnerabilities, these vulnerabilities can be thus exploited, and overall, such exploitation outweighs the advantages provided by obscurity.

9 "Fact Sheet: The U.S. Election Assistance Commission's Voting System Testing and Certification Program," *U.S. Election Assistance Commission*, last modified March 7, 2017, https://www.eac.gov/news/2017/03/07/fact-sheet-the-us-election-assistance-commissions-voting-system-testing-and-certification-program-voting-systems-certification-communications-fact-sheet.

10 See, for example, Mark Niesse, "How to hack elections on Georgia's electronic voting machines: Demonstration shows malware could change election results," *The Atlanta Journal-Constitution*, last modified April 18, 2018, https://www.ajc.com/news/state--regional-govt--politics/how-hack-elections-georgia-electronic-voting-machines/K4s5F935330BS6fGDm3CVI/.

11 "The Verifier – Polling Place Equipment – November 2018," *Verified Voting*, accessed April 16, 2019, https://www.verifiedvoting.org/verifier/#.

12 Jordan Wilkie, "America's new voting machines bring new fears of election tampering," *The Guardian*, April 22, 2019, https://www.theguardian.com/us-news/2019/apr/22/us-voting-machines-paper-ballots-2020-hacking?CMP=share_btn_tw.

13 Ibid.

14 Ibid.

15 Joseph Anthony, "The Importance of Updating the Help America Vote Act," *Scholars Strategy Network*, February 9, 2017, https://scholars.org/brief/importance-updating-help-america-vote-act.

16 National Academies, *Securing the Vote: Protecting American Democracy*, National Academies Press, 2018.

17 In a risk-limiting audit, a percentage of electronic vote counts would be audited using the VVPAT depending on the closeness of the reported outcome—for close races, a greater percentage of votes are audited, but with wide margins of victory, a smaller percentage would be called for.

18 "Protecting American Votes and Elections Act of 2018," *Ron Wyden: United States Senator for Oregon*, accessed April 16, 2019, https://www.wyden.senate.gov/imo/media/doc/PAVE%20Act%20of%202018%20UPDATED.pdf

19 Ibid.

20 For example, the Harvard Kennedy School of Government has published a Campaign Cybersecurity Playbook that suggests cybersecurity recommendations for political campaigns. See "The Cybersecurity Campaign Playbook: Defending Digital Democracy," *Harvard Kennedy School*, May 2018, https://www.belfercenter.org/sites/default/files/files/publication/CampaignPlaybook_0.pdf.

21 The recommendations in the Harvard Kennedy School of Government's Campaign Cybersecurity Playbook are also applicable to those who work on election administration.

22 As one illustration of such a partisan leaning, in 2003, the CEO of a vendor trying to sell voting machines in Ohio said that he was "committed to helping Ohio deliver its electoral votes to the president next year." See Julie Carr Smyth, "Voting Machine Controversy," *Cleveland Plain Dealer*, August 28, 2003, https://www.commondreams.org/headlines03/0828-08.htm.

23 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as Critical Infrastructure Subsector," *U.S. Department of Homeland Security*, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

CHAPTER THREE

1 "Internet Agency Indictment," *U.S. Department of Justice*, filed February 16, 2018, https://www.justice.gov/file/1035477/download.

2 Alex Stamos, "An Update on Information Operations on Facebook," *Facebook Newsroom*, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update.

3 For decades, social scientists have been attempting to estimate the causal influence of campaign advertising on electoral outcomes, but with limited success. See Jörg L. Spenkuch and David Toniatti, "Political Advertising and Election Results," *The Quarterly Journal of Economics* 133, no. 4 (November 2018): 1981-2036, https://doi.org/10.1093/qje/qjy010; Avi Ben-Bassat, Momi Dahan, and Esteban F. Klor, "Does campaign spending affect electoral outcomes?" *Electoral Studies* 40 (December 2015): 102-114, https://doi.org/10.1016/j.electstud.2015.06.012.

4 4/19/16 Facebook Advertisement ID 6045151094235.

5 Senator Amy Klobuchar, "S.1989 – Honest Ads Act," *Congress.gov*, https://www.congress.gov/bill/115th-congress/senate-bill/1989.

6 "Governor Cuomo Signs the New York State Democracy Protection Act to Secure the Integrity of New York Elections," *New York State: Governor Andrew M. Cuomo*, April 18, 2018, https://www.governor.ny.gov/news/governor-cuomo-signs-new-york-state-democracy-protection-act-secure-integrity-new-york.

7 Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?" *The New York Times*, September 2, 2018, https://www.nytimes.com/2018/09/02/technology/03adarchive.html.

8 "Facebook and Google: This is What an Effective Ad Archive API Looks Like," *Mozilla Blog*, March 27, 2019, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/.

CHAPTER FOUR

1 Natalka Pisnia, "Why Has RT Registered as a Foreign Agent with the US?" *BBC*, November 15, 2017, http://www.bbc.com/news/world-us-canada-41991683.

2 Edward Delman, "When is a TV Channel a Foreign Agent?" *The Atlantic*, April 22, 2015, https://www.theatlantic.com/international/archive/2015/04/rt-lobbyist-russia-putin-media/390621/.

3 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html?_r=0.

4 Ibid.

5 Julia Ioffe, "What is Russia Today?" *Columbia Journalism Review*, 2010, https://archives.cjr.org/feature/what_is_russia_today.php

6 David Cloud, Tracy Wilkinson, and Joseph Tanfani, "FBI Investigates Russian Government Media Organizations Accused of Spreading Propaganda in U.S." *The LA Times*, 2017, https://www.latimes.com/nation/la-na-russia-propaganda-20170913-story.html; James Vincent,"Russia Today news anchor Liz Wahl resigns live on air in response to "whitewashed" Ukraine coverage," *The Independent*, 2014, https://www.independent.co.uk/news/world/russia-today-anchor-resigns-lives-on-air-in-response-to-whitewashed-ukraine-coverage-9172818.html.

7 James Vincent,"Russia Today news anchor Liz Wahl resigns live on air in response to 'whitewashed' Ukraine coverage," *The Independent,* 2014, https://www.independent.co.uk/news/world/russia-today-anchor-resigns-lives-on-air-in-response-to-whitewashed-ukraine-coverage-9172818.html.

8 Ibid.

9 Ibid.

10 Statements from several interviews, as quoted in: Ben Nimmo, "Question That: RT's Military Mission," *Digital Forensic Research Lab,* 2018, https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88.

11 U.S. Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," *ICA,* 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

12 Danielle Ryan, "RT America Was Not 'Pro-Trump'," *The Nation,* 2017, https://www.thenation.com/article/rt-america-was-not-pro-trump/; Ben Nimmo, "Understanding the Role of Russian Propaganda in the US Election," *New Atlanticist,* 2016, https://www.atlanticcouncil.org/blogs/new-atlanticist/understanding-the-role-of-russian-propaganda-in-the-us-election.

13 "Photo of Clinton having trouble with stairs fuels rumors of bad health," *RT,* August 8, 2016, retrieved at https://www.rt.com/usa/355047-clinton-stairs-health-problem/.

14 "#PayToPlay: Hillary Clinton faces corruption scandal after links between donors & State Department exposed," *RT,* August 10, 2016, retrieved at https://www.rt.com/usa/355447-clinton-emails-state-department-foundation/.

15 Pepe Escobar, "Hillary, Queen of War: The Road Map Ahead," *Sputnik International,* August 4, 2016, https://sputniknews.com/columnists/201608041043937453-hillary-clinton-war-queen/.

16 See, e.g., RT America, "Watching the Hawks: The Nation Endorses Bernie Sanders," *YouTube,* January 18, 2016, https://www.youtube.com/watch?v=hZL-ztfeVIA.

17 Philip Howard, Bharath Ganesh, Dimitria Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Project,* 2018, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

18 Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet is an Online News Giant. YouTube Helped," *The New York Times,* 2017, https://www.nytimes.com/2017/10/23/technology/youtube-russia-rt.html;"RT Leads Among TV News Channels on YouTube with 5 Billion Views," *RT News,* 2017, https://www.rt.com/about-us/press-releases/rt-youtube-5bn-views/.

19 RT America, "Secret World of US Election: Julian Assange Talks to John Pilger," *YouTube,* November 5, 2016, https://www.youtube.com/watch?v=_sbT3_9dJY4.

20 Jack Nicas, "Russian State News Site Thrives on YouTube, Facebook," *The Wall Street Journal,* 2017, https://www.wsj.com/articles/russia-state-news-outlet-rt-thrives-on-youtube-facebook-1508808937.

21 Robert M. Faris, Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler, "Partisanship, Propaganda and Disinformation: Online Media and the 2016 U.S. Presidential Election," *Berkman-Klein Center For Internet & Society Research Paper,* 2017.

22 Megan Metzger and Steven Wilson, "The Other Russian Strategy: RT and the U.S. Midterms," Unpublished Working Paper, 2018.

23 Andrew Osborn and Christian Lowe, "Russian names nine U.S.-backed news outlets likely to be labeled 'foreign agents,' *Reuters,* November 16, 2017, https://www.reuters.com/article/us-russia-usa-media-restrictions-idUSKBN1DG25N.

24 Jeanne Whalen and David Crawford, "How WikiLeaks Keeps its Funding Secret," *The Wall Street Journal,* updated August 23, 2010, https://www.wsj.com/articles/SB10001424052748704554104575436231926853198.

25 Pisnia.

26 Motion to Dismiss or Affirm, Bluman v. FEC, No. 11-275, slip op. at 2 (2011).

27 Ibid.

28 Ibid., 3 (quoting Act of July 4, 1966, Pub. L. No. 89-386, § 8(a) (originally codified at 18 U.S.C. 613 (1970)).

29 See ibid., § 611(c). The definition includes other actions less applicable to this paper.

30 Ibid., § 611(d).

31 Ibid., § 612(a).

32 Ibid., § 612(a)(1)-(10).

33 Ibid., § 614(b).

34 Ibid., § 615.

35 See Cynthia Brown, "The Foreign Agents Registration Act (FARA): A Legal Overview," *Congressional Research Service*, December 4, 2017.

36 See Pub. L. 104-65 § 9(1)(A) (1995).

37 Meese v. Keene, 481 U.S. 465 (1987).

38 Ibid. China Daily is a Chinese "state-run English-language newspaper" that is "widely available". See Bethany Allen-Ebrahimian and Elias Groll, "China's Flagship TV Network Hasn't Registered as a Foreign Agent," *Foreign Policy*, December 19, 2017, http://foreignpolicy.com/2017/12/19/why-isnt-chinas-flagship-tv-network-registered-as-a-foreign-agent-fara-russia-cctv-america-beijing/.

39 Bill Chappell, "TV Company Linked To Russia's RT America Registers As Foreign Agent In U.S.," *Reuters*, November 14, 2017, https://www.npr.org/sections/thetwo-way/2017/11/14/564045159/rt-america-firm-registers-as-foreign-agent-in-u-s-russia-looks-to-retaliate.

40 "Production Company Registers Under the Foreign Agent Registration Act as Agent for the Russian Government Entity Responsible for Broadcasting RT," *U.S. Department of Justice*, November 13, 2017, https://www.justice.gov/opa/pr/production-company-registers-under-foreign-agent-registration-act-agent-russian-government.

41 Hadas Gold, "Russia's RT American registers with DOJ as a foreign agent," *CNN Money*, November 13, 2017, https://money.cnn.com/2017/11/13/media/russia-rt-fara/index.html.

42 Twitter Public Policy, "Announcement: RT and Sputnik Advertising," *Twitter Public Policy Blog*, 2017, https://blog.twitter.com/en_us/topics/company/2017/Announcement-RT-and-Sputnik-Advertising.html. In retaliation, RT published documents showing Twitter's offer to sell *RT* up to a 15% "share of voice" (SOV) in their election-based advertising prior to the 2016 elections, although it seems that *RT* did not accept the proposal. See Alex Kantrowitz, "Twitter Offered Russian Television Network RT 15% of Its Total Share of US Election Advertising," *Buzzfeed News*, 2017, https://www.buzzfeednews.com/article/alexkantrowitz/twitter-offered-rt-15-of-its-total-share-of-us-elections.

43 Elizabeth Dwoskin, "Twitter bans Russian government-owned news sites RT and Sputnik from buying ads," *The Washington Post*, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/10/26/twitter-bans-russian-government-news-sites-rt-and-sputnik-from-buying-ads/?noredirect=on&utm_term=.0ce937f95972.

44 Wakabayashi and Confessore.

45 Alexandra Ma, "Russia's RT attacks Facebook for suspending 4 viral news channels that broadcast Kremlin talking points to millennials," *Business Insider*, 2019, https://www.businessinsider.com/rt-attacks-facebook-for-suspending-in-the-now-soapbox-other-pages-2019-2.

46 Alina Polyakova, "The Kremlin's Latest Crackdown on Independent Media: Russia's New Foreign Agent Law in Context," *Foreign Affairs*, December 5, 2017, https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/kremlins-latest-crackdown-independent-media.

CHAPTER FIVE

1 Alex Stamos, "An Update on Information Operations on Facebook," *Facebook Newsroom,* September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update.

2 Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan," *Facebook Newsroom,* April 1, 2019, https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/; Nathaniel Gleicher, "Removing More Coordinated Authentic Behavior From Russia," *Facebook Newsroom,* May 6, 2019, https://newsroom.fb.com/news/2019/05/more-cib-from-russia/.

3 Alexandra Ma, "Russia's RT attacks Facebook for suspending 4 viral news channels that broadcast Kremlin talking points to millennials," *Business Insider,* 2019, https://www.businessinsider.com/rt-attacks-facebook-for-suspending-in-the-now-soapbox-other-pages-2019-2.

4 Cameron F. Kerry, "A federal privacy law could do better than California's," *Los Angeles Times,* April 25, 2019, https://www.latimes.com/opinion/op-ed/la-oe-kerry-ccpa-data-privacy-laws-20190425-story.html.

5 Kathleen Hall Jamieson, *CYBERWAR: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know* (Oxford University Press, 2018).

6 Special Counsel Robert S. Mueller, III., "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," *U.S. Department of Justice,* March 2019, 42.

7 Tony Biasotti, "Reports shouldn't profile mass shooters, say experts," *Columbia Journalism Review,* August 31, 2018, https://www.cjr.org/united_states_project/jacksonville-shooting-contagion.php; Cindi Deutschman-Ruiz, "Reporting on Suicide," *Poynter,* November 11, 2003, https://www.poynter.org/archive/2003/reporting-on-suicide/.

8 Dipayan Ghosh and Ben Scott, "The Technologies Behind Precision Propaganda on the Internet," 2018.

9 "Standards, Guidelines & Best Practices," *Internet Advertising Bureau,* https://www.iab.com/guidelines/.

10 Bethany Shiner, "Self-Regulation Is Not Enough: The Law on Micro-Targeted Online Political Campaigns and Big Data Needs Reform," *Democratic Audit,* February 4, 2019, http://www.democraticaudit.com/2019/02/04/self-regulation-is-not-enough-the-law-on-micro-targeted-online-political-campaigns-and-big-data-needs-reform/.

11 Hamsini Sridharan, "Principles and Policies to Counter Deceptive Digital Politics," *Maplight,* February 12, 2019, https://maplight.org/story/principles-and-policies-to-counter-deceptive-digital-politics/; Dipayan Ghosh and Ben Scott, "Digital Deceit II: Executive Summary," *New America,* https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/executive-summary/.

12 Howard et al.

13 *CrowdTangle,* 2019, https://www.crowdtangle.com/.

14 Kai-Cheng Yang, Onur Varol, Clayton A. Davis, Emilio Ferrara, Alessandro Flammini, and Filippo Mencz, "Arming the public with artificial intelligence to counter social bots," *Human Behavior and Emerging Technologies* 1 (2019): 48– 61, https://doi.org/10.1002/hbe2.115; Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, "Detecting Bots on Russian Political Twitter," *Big Data* 5, no. 4 (2017): 310-324, http://dx.doi.org/10.1089/big.2017.0038.

15 Jamie Fly, Laura Rosenberger, and David Salvo, "Policy Blueprint for Countering Authoritarian Interference in Democracies," *The Alliance for Securing Democracy/German Marshall Fund,* http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

16 Timothy Garton Ash, Robert Gorwa, and Danaë Metaxa, "GLASNOST! Nine ways Facebook can make itself a better forum for free speech and democracy," *Reuters Institute,* https://reutersinstitute.politics.ox.ac.uk/our-research/glasnost-nine-ways-facebook-can-make-itself-better-forum-free-speech-and-democracy.

17 "Disinformation and 'fake news': Final Report," *House of Commons, Digital, Culture, Media and Sport Committee,* https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/; Sridharan.

18 ISAO Standards Organization, 2019, https://www.isao.org.

19 Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," *New Knowledge,* 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

20 See Electricity Information Sharing and Analysis Center, https://www.eisac.com/, and Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.

21 Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, "The Use of Twitter Bots in Russian Political Communication," *PONARS Eurasia Policy Memo No. 564*, 2019, http://www.ponarseurasia.org/memo/use-twitter-bots-russian-political-communication.

22 Sam Stein, Jackie Kucinich, and Scott Bixby, "Trump Won't Rule Out Using Stolen Data in 2020 Campaign," *The Daily Beast,* February 21, 2019, https://www.thedailybeast.com/every-2020-candidate-but-trump-promises-no-stolen-data.

23 Sam Wineburg and Sarah McGrew, "Lateral Reading: Reading Less and Learning More When Evaluating Digital Information," *Stanford History Education Group Working Paper No. 2017-A1*, October 2017, http://dx.doi.org/10.2139/ssrn.3048994.

24 Gordon Pennycook and David Rand, "Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking," *Journal of Personality* (2019): 1–16, https://doi.org/10.1111/jopy.12476.

25 Sergei M. Guriev and Daniel Treisman, "Informational Autocrats," July 2018, http://dx.doi.org/10.2139/ssrn.3208523.

26 To put it differently, Western democracies need to update *The Open Society and Its Enemies* for the age of digital globalization.

27 Henry John Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy," *Berkman Klein Center Research Publication No. 2018-7*, October 2018, http://dx.doi.org/10.2139/ssrn.3273111.

28 See the following for an example of a comprehensive course at the college student level: https://webliteracy.pressbooks.com/.

29 European Commission, "A Multi-Dimensional Approach to Disinformation," *Report of the Independent High-Level Group on Fake News and Online Disinformation,* 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, 27.

30 Andrew Guess, Jonathan Nagler, and Joshua Tucker, "Less than you think: Prevalence and predictors of fake news dissemination on Facebook," *Science Advances* 5, no. 1, 2019, https://advances.sciencemag.org/content/5/1/eaau4586.

CHAPTER SIX

1 Matt A. Vega, "The First Amendment Lost in Translation: Preventing Foreign Influence in U.S. Elections After Citizens United v. FEC," 44 Loy. L.A. L. Rev. 951, 2011, https://digitalcommons.lmu.edu/llr/vol44/iss3/3.

2 The conviction of Russian national Marina Butina for her activities to cultivate contacts with the American National Rifle Association is a most recent example. She was convicted in April 2019 for failing to register as a foreign agent under FARA.

3 Karen Yourish and Larry Buchanan, "Mueller Report Shows Depth of Connections Between Trump Campaign and Russians," *The New York Times,* April 19, 2019, https://www.nytimes.com/interactive/2019/01/26/us/politics/trump-contacts-russians-wikileaks.html.

4 Rosalind S. Helderman, Tom Hamburger, Kevin Uhrmacher, and John Muyskens, "The making of the Steele dossier," *The Washington Post,* February 6, 2018, https://www.washingtonpost.com/graphics/2018/politics/steele-timeline/?noredirect=on&utm_term=.c6e72506b3d9.

5 Rosalind S. Helderman and Spencer S. Hsu, "American political consultant admits foreign money was funneled to Trump inaugural," *The Washington Post,* September 1, 2018, https://www.washingtonpost.com/local/public-safety/washington-consultant-for-ukraine-party-set-to-plead-guilty-to-violating-lobbyist-disclosure-law/2018/08/31/172cf2c8-ad23-11e8-a8d7-0f63ab8b1370_story.html?noredirect=on&utm_term=.65ba62128243.

6 Jonathan Swan and Harper Neidig, "Trump campaign solicits illegal foreign donations despite warnings," *The Hill,* July 16, 2016, https://thehill.com/homenews/campaign/288031-trump-campaign-solicits-illegal-foreign-donations-despite-warnings.

CHAPTER SEVEN

1 Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," *Oxford Internet Institute, Computational Propaganda Research Project,* http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf; Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," *Freedom House,* https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism; David Wemer, "Has Progress Been Made in Containing Disinformation?" *Atlantic Council* April 28, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/has-progress-been-made-in-containing-disinformation; and Matt Apuzzo and Adam Atarioano, "Hackers Sow Discord as Vote Looms in Europe," *New York Times,* 1.

2 "Cyber Norms Index," *Carnegie Endowment for International Peace,* https://carnegieendowment.org/publications/interactive/cybernorms.

3 Article 21: "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." See "Universal Declaration of Human Rights," *United Nations,* https://www.un.org/en/universal-declaration-human-rights/index.html.

4 Article 1 assures self-determination to all peoples. Article 25 states in part: "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in Article 2 and without unreasonable restrictions:(a) To take part in the conduct of public affairs, directly or through freely chosen representatives; (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors." "Universal Declaration of Human Rights," *United Nations,* https://www.un.org/en/universal-declaration-human-rights/index.html.

5 Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

6 Michael N. Schmitt, ed., *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

7 "Aims and Priorities," *Freedom Online Coalition,* https://freedomonlinecoalition.com/about-us/about/.

8 A/HRC/RES/20/8: The promotion, protection and enjoyment of human rights on the Internet.

9 For example, these include the Global Commission on the Stability of Cyber Space and the Transatlantic Commission on Election Integrity.

10 Daniel Twining and Kenneth Wollak, "Russia's Nefarious Meddling is Nothing Like Democracy Assistance," *The Washington Post,* April 10, 2018, https://www.washingtonpost.com/opinions/russias-nefarious-meddling-is-nothing-like-democracy-assistance/2018/04/10/b8942f20-3ce2-11e8-a7d1-e4efec6389f0_story.html?utm_term=.4381b8f7a0e2.

11 Jack Goldsmith, "Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference with Putin," *Lawfare,* July 16, 2018, https://www.lawfareblog.com/uncomfortable-questions-wake-russia-indictment-20-and-trumps-press-conference-putin.

12 Joshua Geltzer and Jake Sullivan, "How to Prevent the Next Election Disaster," *Politico,* January 22, 2019, https://www.politico.com/magazine/story/2019/01/22/prevent-election-disaster-224032.

13 "Warsaw Declaration: Toward a Community of Democracies," *Community of Democracies,* June 27, 2000, https://community-democracies.org/app/uploads/2017/02/2000-Warsaw-Declaration-ENG.pdf.

14 "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations General Assembly,* July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

15 "The Pledge for Election Integrity," *Alliance for Democracies: Transatlantic Commission on Election Integrity,* 2019, https://electionpledge.eu.

16 See "Universal Declaration of Human Rights".

17 "Norm Package Singapore," *Global Commission on the Stability of Cyberspace*, November 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

18 Toomas Hendrik Ilves, "A Digital Defense Alliance," *Berlin Policy Journal*, January 10, 2018, https://berlinpolicyjournal.com/a-digital-defense-alliance.

CHAPTER EIGHT

1 See, for example, "Ukraine and Russia Sanctions," *U.S. Department of State*, https://www.state.gov/e/eb/tfs/spi/ukrainerussia/; "Ukraine-/Russia-related Sanctions," *U.S. Department of the Treasury*, https://www.treasury.gov/resource-center/sanctions/Programs/pages/ukraine.aspx. See also Executive Orders 13660, 13685, 13694, 13757, int. al. For sanctions legislation see Countering America's Adversaries Through Sanctions Act (CAATSA), PL 115-44; Ukraine Freedom Support Act of 2014 (UFSA); Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (SSIDES); International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706; National Emergencies Act (NEA), 50 U.S.C. §§ 1601-1651. For the most recent (as of publication) update to the list of "Specifically Designated Nationals" related to Russia sanctions by the U.S. Office of Foreign Assets Control (OFAC), see "Specifically Designated Nationals List Update," *U.S. Department of the Treasury, Office of Foreign Assets Control*, March 15, 2019, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190315.aspx.

2 In a press conference on April 19, 2019, Secretary of State Mike Pompeo responded to questions about the Special Counsel report saying, "We will make very clear to them [the Russians] that this is unacceptable behavior... We will take tough actions which raise the cost for Russian malign activities. And we will continue to do that" as quoted in "Mueller probe over, but little chance for US-Russia reconciliation," *Agence France-Presse (AFP) wire service*, April 19, 2019, https://www.france24.com/en/20190419-mueller-probe-over-but-litte-chance-us-russia-reconciliation. For a detailed listing of how Trump has described Putin and Russian meddling in the five years up to the July 2018 Helsinki Summit, see Erica R. Hendry, "The many different ways Trump has described Putin and Russian election interference," *PBS NewsHour*, July 16, 2018, https://www.pbs.org/newshour/politics/the-many-different-ways-trump-has-described-putin-and-russian-election-interference.

3 Specifically, referring to reports that U.S. Cyber Command "basically took the [St. Petersburg-based Russian Internet Research Agency] offline" during the day of the 2018 midterms. See Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

4 With respect to deterring nation state malicious cyber actions more generally, see Christopher Painter, "Deterrence in cyberspace: Spare the costs, spoil the bad state actor: Deterrence in cyberspace requires consequences," *Australia Strategic Policy Institute, International Cyber Policy Centre Policy Paper*, 2018, https://www.aspi.org.au/report/deterrence-cyberspace.

5 The authors recognize the multiple forms of deterrence contained in the security literature, including deterrence by denial, entanglement, and norms, in addition to deterrence by cost-imposition (often called punishment.) We emphasize here only the last form of deterrence. What constitutes in effect these other aspects of deterrence are addressed in other chapters of this paper, especially those on election infrastructure security and international norms.

6 Eric Schmitt, David E. Sanger, and Maggie Haberman, "In Push for 2020 Election Security, Top Official Was Warned: Don't Tell Trump," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/us/politics/russia-2020-election-trump.html.

7 See Bernard Brodie, *Strategy in the Missile Age* (Princeton University Press, 1959); Thomas Schelling, *The Strategy of Conflict* (Harvard University Press, 1960); and Herman Kahn, *On Thermonuclear War* (Princeton University Press, 1960), among additional literature.

8 More recent work since the end of the Cold War, drawing on findings from cognitive psychology such as Tversky and Kahneman's work on prospect theory, has shown how cognitive biases inhibit rational decision-making. For example, loss-aversion (or defense of perceived status-quo) has been found more likely to lead to conflict than otherwise rationally-equivalent gain-seeking. See Robert Jervis, "Political Implications of Loss Aversion," *Political Psychology* 13, no. 2, June 1992, 187-204, https://www.researchgate.net/publication/271785014_Political_Implications_of_Loss_Aversion.

9 "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," *The White House*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. See also Christopher Painter, "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," *U.S. Department of State*, May 25 2016, https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

10 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," *U.S. Department of State*, May 31, 2018, https://www.state.gov/s/cyberissues/eo13800/282011.htm.

11 Nakashima.

12 Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

13 The new Commander's vision of U.S. Cyber Command involves persistent engagement and defending forward. Under this direction, the new authorities have reportedly permitted U.S. Cyber Command to engage in certain offensive cyber operations under certain circumstances without direct White House approval. Nevertheless, advocates of these and similarly related changes have not yet publicly acknowledged that they entail additional cyber risk, compared to a strategy based on cyber restraint.

14 When the President undercuts the messaging, such as the current President casting doubt on whether Russia interfered with U.S. elections, that alone undercuts even the best efforts and actions of others in the government. Of course, no one can force a president to take a particular factual stand, and it may be that we will need to wait for a future president to robustly condemn Russia's actions, but tools such as mandatory sanctions help alleviate that issue.

15 "Defending Elections against Trolls from Enemy Regimes (DETER)" (S.2785), https://www.congress.gov/115/bills/s2785/BILLS-115s2785is.pdf.

16 "Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats," *U.S. Department of State*, May 31, 2018.

17 Pursuant to its new deterrence initiative, the U.S. Department of State and the interagency are currently developing a list of potential consequences that provide a menu of options for responding to malicious state cyber conduct. In addition, the State Department is bringing in a range of U.S. allies and partners to discuss the program and considering ways to communicate warnings of potential consequences to adversaries in advance of an attack. Though admittedly difficult, this work should be completed as soon as possible.

18 To illustrate, sanctions for activities related to the situation in Ukraine (but unrelated to election interference) were undertaken by the Obama Administration in 2014. At that time, the following individuals were designated by the U.S. Treasury because each is controlled by, has acted for or on behalf of, or has provided material or other support to, a senior Russian government official: Gennady Timchenko (a founder of Gunvor, an independent commodity trading company involved in the oil and energy markets), Arkady Rotenberg and Boris Rotenberg (executors of contracts for the Sochi Olympic Games and Gazprom), and Yuri Kovalchuk (largest single shareholder of Bank Rossiya and personal banker for senior officials of the Russian Federation). Bank Rossiya (the personal bank for senior officials of the Russian Federation) was designated for the same reasons. Assets of designated entities within U.S. jurisdictions are frozen, and transactions by U.S. persons or within the United States involving designated individuals and entities are generally prohibited. See "Treasury Sanctions Russian Officials, Members of the Russian Leadership's Inner Circle, And An Entity For Involvement In The Situation In Ukraine," *U.S. Department of the Treasury*, March 20, 2014, https://www.treasury.gov/press-center/press-releases/Pages/jl23331.aspx.

19 The EU Cyber Diplomacy Toolbox that authorizes economic sanctions at the EU level for malicious cyber actions is a good example. See, for example, Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" *European Union Institute for Security Studies*, July 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

20 For the outline of a comprehensive strategy for dealing with Russia today, see Michael McFaul, "Russia as It Is: A Grand Strategy for Confronting Putin," *Foreign Affairs* 97, no. 4, (July-August 2018), 82-91.

ABOUT THE AUTHORS

Allison Berke is Executive Director of the Stanford Cyber Initiative at the Freeman Spogli Institute for International Studies (FSI) at Stanford University, where she manages research, education, and outreach activities related to the secure integration of cyber technologies into society.

Larry Diamond is Principal Investigator of the Global Digital Policy Incubator (GDPi) at FSI's Cyber Policy Center; Senior Fellow at FSI; Senior Fellow at the Hoover Institution; and Professor, by courtesy, of Political Science and Sociology at Stanford University. He is founding co-editor of the Journal of Democracy and serves as Senior Consultant at the International Forum for Democratic Studies of the National Endowment for Democracy.

Eileen Donahoe is Executive Director of GDPi, former U.S. Ambassador to the United Nations Human Rights Council in Geneva, and former Director of Global Affairs at Human Rights Watch. Eileen is a member of the Board of Directors of the National Endowment for Democracy; the World Economic Forum Council on Digital Economy and Society; the University of Essex Advisory Board on Human Rights, Big Data and Technology; the Dartmouth College Board of Trustees, and the Council on Foreign Relations. She is a Distinguished Fellow at the Center for International Governance Innovation.

Andrew Grotto is Director of the Cyber Policy Center's Program on Geopolitics, Technology, and Governance; a William J. Perry International Security Fellow at CISAC at FSI; and a Research Fellow at the Hoover Institution. Prior to Stanford, Grotto was the Senior Director for Cybersecurity Policy at the White House in both the Obama and Trump administrations, where he served as a principal architect of President Obama's Cybersecurity National Action Plan and President Trump's cybersecurity executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure".

Toomas Ilves is a GPDi Fellow, Distinguished Visiting Fellow at the Hoover Institution, and Berggruen Fellow at the Center for Advanced Studies in the Behavioral Sciences at Stanford University. He was elected President of the Republic of Estonia in 2006 and re-elected for a second term in 2011, during which he was appointed to serve in several high positions in the field of ICT in the European Union. He served as chairman of the EU Task Force on eHealth from 2011 to 2012 and chairman of the European Cloud Partnership Steering Board from 2012 to 2014. From 2014 to 2015, he was the co-chair of the advisory panel of the World Bank's World Development Report 2016 "Digital Dividends" and chair of the World Economic Forum's Global Agenda Council on Cyber Security beginning in June 2014.

Bronte Kass is the Program Manager for FSI Director Michael McFaul at Stanford University.

Zachary Krowitz is a Research Assistant for Professor Nate Persily and student at Stanford Law School.

Herbert Lin is a Senior Research Scholar at CISAC; Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution; and former Chief Scientist of the Computer Science and Telecommunications Board, National Research Council of the National Academies. He is also an Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University, a member of the Science and Security Board of the Bulletin of Atomic Scientists, and a member of the Aspen Institute Cybersecurity Group.

Michael McFaul is the Director of FSI; the Ken Olivier and Angela Nomellini Professor of International Studies, Department of Political Science; and Peter and Helen Bing Senior Fellow at the Hoover Institution, all at Stanford University. He also works as an analyst for NBC News and writes a monthly column for The Washington Post. He served five years in the Obama administration, first as Special Assistant to the President and Senior Director for Russian and Eurasian Affairs at the National Security Council at the White House from 2009-12), and then as U.S. Ambassador to the Russian Federation from 2012-14. He has authored several books, including most recently The New York Times bestseller From Cold War to Hot Peace: An American Ambassador in Putin's Russia (2018).

Megan Metzger is a Research Scholar at FSI and Associate Director for Research at GDPi at Stanford University.

Chris Painter is a William J. Perry Fellow at FSI, Commissioner on the Global Commission for the Stability of Cyberspace, former Coordinator for Cyber Issues for the Department of State, and former White House Senior Director for Cybersecurity Policy. He was named the Bartels World Affairs Fellow for 2017-18 by Cornell University and awarded the Order of the Rising Sun in 2018 by the Government of Japan for promoting Japan-U.S. Cyber collaboration.

Nate Persily is Co-Director of the Cyber Policy Center; Senior Fellow at FSI; James B. McClatchy Professor of Law at Stanford Law School; and Professor, by courtesy, of Communication and Political Science. He is co-author of the leading election law casebook, The Law of Democracy (2016). He has served as the Research Director of the Presidential Commission on Election Administration, as a court-appointed Special Master for the redistricting process in numerous states, and on the National Academy of Sciences Committee on The Future of Voting. In recognition of his current work examining the impact of changing technology on political communication, campaigns, and election administration, he has been honored as an Andrew Carnegie Fellow, a Fellow at the Center for Advanced Study in the Behavioral Sciences, and as a commissioner on the Kofi Annan Commission on Elections and Democracy in the Digital Age.

Sergey Sanovich is a Cyber Postdoctoral Fellow at CISAC at Stanford University. His report, commissioned by the Oxford Internet Institute, on the domestic origins of Russian government's disinformation campaigns abroad was published in an Oxford University Press volume on computational propaganda in November 2018.

Alex Stamos is Director of the Cyber Policy Center's Internet Observatory, an Adjunct Professor at FSI, and a visiting scholar at the Hoover Institution. Prior to joining Stanford, Alex served as the Chief Security Officer of Facebook, where he led the company's investigation into manipulation of the 2016 U.S. presidential election and helped pioneer several successful protections against these new classes of abuse. In April 2017, he co-authored "Information Operations and Facebook", a highly cited examination of the influence campaign against the U.S. election.

ABOUT THE STANFORD CYBER POLICY CENTER

The **Stanford Cyber Policy Center** at the Freeman Spogli Institute is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance, and public policy. Through research, policy engagement, and teaching, the Stanford Cyber Policy Center seeks to bring cutting-edge insights and solutions to national governments, international institutions, and industry with its four principal programs. Professors Dan Boneh and Nate Persily are co-directors of the Center.

1. The **Global Digital Policy Incubator** (GDPi) is a multi-stakeholder collaboration hub for the development of norms and policies to protect human rights, civic space, and democratic processes in digital society. GDPi evaluates the human-rights impacts of digital technologies themselves, as well as the impacts of policy and regulatory responses to technology, with particular emphasis on risks to free expression, privacy, security, and democratic engagement. Larry Diamond and Eileen Donahoe are co-directors of this program.

2. The **Program on Geopolitics, Technology, and Governance** (GTG) is dedicated to world-class scholarly and policy-oriented research on the political, legal, and economic implications of digital innovation and global competition. Andrew Grotto is director of this program.

3. The **Stanford Internet Observatory** is a cross-disciplinary program of research, teaching, and policy engagement for the study of abuse in current information technologies, with a focus on social media. In addition, the Observatory was created to develop a novel curriculum on trust and safety that is a first in computer science, and to translate research discoveries into training and policy innovations for the public good. Alex Stamos is director of this program.

4. The **Program on Democracy and the Internet** (PDI) produces research, hosts events and convenings, and teaches current and future leaders about the challenges that new technologies pose to democracy in the digital age. PDI seeks to establish and survey this new field of digital democracy, setting forth what is known and what needs to be discovered, in order to evaluate and promote public, private, and civil society policy responses to address these trends and challenges. Francis Fukuyama, Nate Persily, and Rob Reich are co-directors of this program.

ABOUT THE FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES

The Freeman Spogli Institute for International Studies (FSI) is Stanford University's premier research institute for the study of international affairs. Our Mission is threefold:

1. **Produce world-class, world-wide research** – With 50 appointed faculty, FSI is a hub for Stanford scholars who conduct research across multiple disciplines with an international impact. With a diverse group of seven research centers and 50 programs dedicated to deep investigation of critical global issues, our research topics include governance, security, health, energy, international development, and cyber policy.

2. **Teach and train tomorrow's leaders** – Each year, we educate dozens of graduate students and hundreds of undergraduates in both traditional and innovative ways. Our faculty teach over 65 classes a year and mentor students through guided research. FSI is also home to the Ford Dorsey Master's in International Policy, a two-year master's degree.

3. **Engage policymakers** – Our work provides context for decision-making in Washington, Geneva, Beijing and beyond. FSI's International Policy Lab ensures our research has real-world impact.

In addition to the new Cyber Policy Center, FSI has six research centers that serve as the focal points for the institute's activities:

- The **Center on Democracy, Development and the Rule of Law** (CDDRL) is dedicated to the study of the political and economic institutions that constitute modern liberal democracy. CDDRL's mission is to understand how countries can overcome poverty, instability and abusive rule to become well-governed states. CDDRL's work spans the globe and bridges the divide between academic research and policy analysis, forging partnerships not only with other research centers, but also with international development agencies, governments, and civil society organizations in numerous countries.

- The **Center on Food Security and the Environment** (FSE) is a joint effort of FSI and the Stanford Woods Institute for the Environment. With the goal of designing new approaches to solving global hunger and environmental degradation, FSE is building an evolving research portfolio with a team of experts in scientific, economic, and policy areas that are critical to global food security, such as adapting to climate change, managing aquaculture, raising smallholder farm productivity, and leveraging big data.

- The **Center for International Security and Cooperation** (CISAC) contributes to world peace by addressing critical security challenges, including cybersecurity, nuclear security, biotechnology, and counterterrorism. CISAC is dedicated to world-class teaching, research, and policy impact by training the next generation of scholars and policymakers through an undergraduate honors program, a fellowship program for military service members, and pre- and post-doctoral research opportunities.
- The **Europe Center** (TEC) promotes interdisciplinary research and teaching on Europe and its role in the world. By supporting scholarly and policy dialogue across nearly all of Stanford's schools, TEC serves as a hub for the study of Europe and global affairs.
- **Stanford Health Policy** (SHP) is devoted to improving healthcare and well-being through improved policy worldwide. SHP comprises research groups within FSI and the Stanford University School of Medicine, a worldwide leader in biomedical innovation, research, and precision medicine. The dual affiliation provides access to researchers who span engineering, medicine, and the social sciences—from pediatrics to geriatrics, politics and law, economics, population health, and decision science.
- The **Walter H. Shorenstein Asia-Pacific Research Center** (APARC) focuses on the interdisciplinary study of contemporary Asia, illuminating policy issues critical to both Asia and the United States. Established in 1983, Shorenstein APARC produces outstanding research, educates the next generation of scholars and policymakers, promotes constructive interaction in the pursuit of influencing U.S. policy toward the Asia-Pacific region, and contributes to Asian nations' understanding of issues key to regional cooperation and to their relations with the United States.

DESIGN: ALEXANDER ATKINS DESIGN, INC.

The **Stanford Cyber Policy Center** at the Freeman Spogli Institute for International Studies is Stanford University's premier center for the interdisciplinary study of issues at the nexus of technology, governance, and public policy. Program areas address topics including cybersecurity, election security, misinformation, digital democracy and human rights, artificial intelligence, and emerging technologies. Through research, policy engagement, and teaching, the Cyber Policy Center seeks to bring cutting-edge insights and solutions to national governments, international institutions, and industry.

Stanford | Cyber Policy Center
Freeman Spogli Institute

Encina Hall
616 Serra Mall C100
Stanford University
Stanford, CA 94305-6055
650.723.4581

fsi.stanford.edu/cyber stanford-cyber@stanford.edu Stanford_Cyber

Immediate Resources for Election Infrastructure Cybersecurity

State and local election officials face a never-ending list of things to do and must dos to improve cybersecurity of election infrastructure. Choosing from the diffuse and vast array of products promising to help can be confusing, costly, and time-intensive. But a solution exists: The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) offers cyber expertise, tools, and services at no cost to election officials to augment their arsenal of cybersecurity

CISA offers a broad range of cyber products and services that are free to state and local election officials. These products include network and system assessments, either self-administered or undertaken by CISA staff; alerts and bulletins; best practices; and mitigation and incident response. For information on CISA's cybersecurity services see DHS Election Infrastructure Security Resources Guide.

But state and local election officials can immediately begin to improve their cybersecurity posture through three simple, straightforward steps – and steps 2 and 3 can be done concurrently.

Step 1: Know Your System

Knowing your elections infrastructure means knowing your network and system vulnerabilities and warning signs of strange network behavior – known as "anomalies" – and then knowing what to do about them.

CISA's Cyber Hygiene assessment is a voluntary, FREE scanning of Internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation's overall resiliency.

Administered by CISA staff experts, the assessment is conducted remotely and is fully automated. Scanning begins 48 hours after the execution of a signed vulnerability scanning authorization letter. Election officials begin receiving weekly assessment results detailing current and previously mitigated vulnerabilities, high-risk hosts, and other port, device and network attributes that organizations working to improve their cybersecurity posture should examine. The report also provides recommended mitigations for each vulnerability discovered via the scanning process. For more information and to arrange the assessment, contact nccicustomerservice@hq.dhs.gov.

Step 2: Know Your Staff Needs To Withstand Phishing

Fortify your staff to further strengthen your elections infrastructure through CISA's Phishing Campaign Assessment, which measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks.

Administered by CISA staff, the assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and the more personalized spear- phishing attacks. For more information and to arrange the assessment, contact nccicustomerservice@hq.dhs.gov.

Step 3: Join the EI-ISAC

Begin improving your cybersecurity status with information sharing – information sharing is key to security. You can't secure your election infrastructure without knowing the threats to protect against, assets to protect, and how to protect. To join the Elections Infrastructure Sharing and Analysis Center (EI-ISAC) for free, please visit https://learn.cisecurity.org/ei-isac-registration.

This information sharing center was created to serve the election community by providing near real time threat and risk sharing as well as cybersecurity best practices geared towards election officials.

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors. The EI-ISAC supports the election infrastructure community through:

- 24 x 7 x 365 network monitoring
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices

Membership in the EI-ISAC is open to all state, local, tribal, and territorial (SLTT) government organizations and associations that support elections in the United States. CISA encourages state and local elections agencies to use this initiative to harden their elections infrastructure.

From:	**devcenter@pcctg.com**
To:	**Colleen McCormack**
Subject:	Issue:33959 of ElectioNet - NH project and New Hampshire organization was added - Two-Factor Authentication updates (DO NOT EDIT THIS:33959)
Date:	Tuesday, November 27, 2018 12:34:04 PM

Issue ID: 33959
Short desc: Two-Factor Authentication updates

Last changed by	bpothugunta
Reported By	bpothugunta
Reported On	2018-11-27 12:32 PM
Tags	
Project	ElectioNet - NH
Organization	New Hampshire
Category	Enhancement
Priority	High
Assigned	bhanu.pothugunta
Status	New
ConvBgId	

comment 353465 posted by bpothugunta on 2018-11-27 12:32 PM, 1 seconds ago

```
Attached some of the changes for 2FA
```

From: devcenter@pcctg.com
To: Colleen McCormack
Subject: Issue:34557 of ElectioNet - NH project and New Hampshire organization was updated - 2FA - Two Factor Authentication (DO NOT EDIT THIS:34557)
Date: Thursday, March 21, 2019 8:52:00 AM

Issue ID: 34557
Short desc: 2FA - Two Factor Authentication

Last changed by	Colleen
Reported By	Colleen
Reported On	2019-03-19 8:45 AM
Tags	
Project	ElectioNet - NH
Organization	New Hampshire
Category	
Priority	High
Assigned	Keval
Status	New
ConvBgId	

comment 359673 posted by Colleen on 2019-03-21 8:50 AM, 0 seconds ago

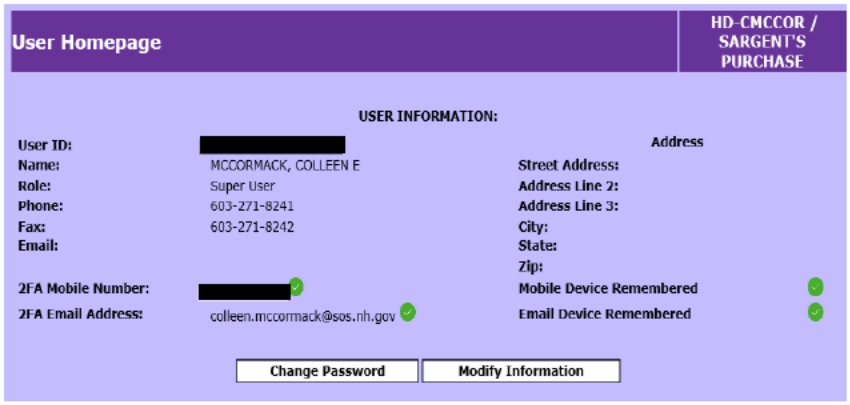
This did not pass. My rememebered device expired today and I was able to log into UAT without any prompt for a code.

changed by Colleen on 2019-03-21 8:50 AM, 0 seconds ago

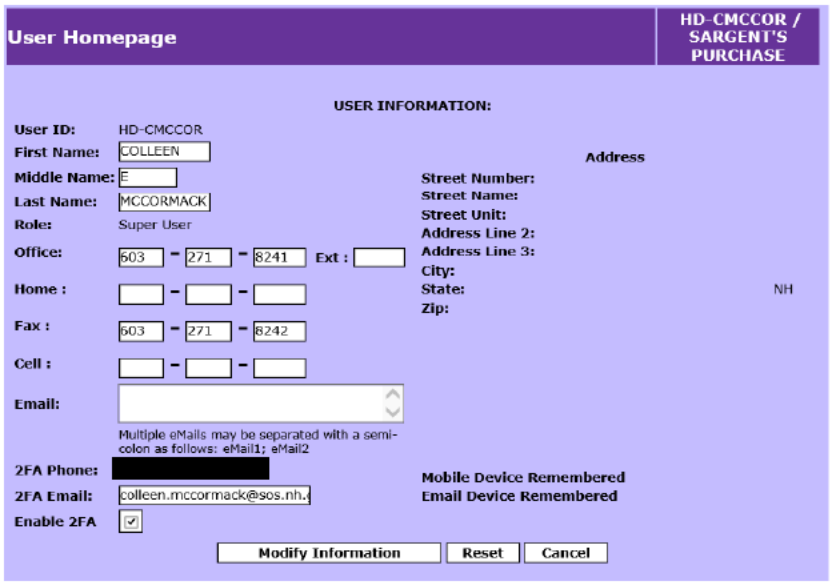
changed module number from "" to "2FA - Two Factor Authentication - Remembered Devices"

comment 359562 posted by Colleen on 2019-03-19 10:08 AM, 1 day and 22 hours ago

I have investigated further and on "My information" screen for the user it still has 2 green check boxes next to Mobile and Email Device Remembered.



On the "User Homepage" where the state enters the information, there are no green check marks, but there is also no text saying "Not Verified"



changed by Colleen on 2019-03-19 10:08 AM, 1 day and 22 hours ago

changed module number from "" to "2FA - Two Factor Authentication - Remembered Devices"

comment 359560 posted by Colleen on 2019-03-19 8:45 AM, 2 days ago

Bhanu,

I set the 2FA to expire the remembered devices for one day. Today is the day it expired. I had it remember my device. Today when I logged into UAT, I went right to the System Reminders screen.

It did not ask me to authenticate or ask me for code. I had done this test once before and I had the same results.

I then went to System -> Maintain TFA -> TFA Settings, I clicked on "Reset" system statewide. This fixed the issue.

ISSUE: I will not know when anyone's remebered device expires. The system should automatically ask them for a code once again and to "Authenticate & remember the device."

I have reset the Remembered device for 7 days.

From: devcenter@pcctg.com
To: Colleen McCormack
Subject: Issue:34557 of ElectioNet - NH project and New Hampshire organization was updated - 2FA - Two Factor Authentication (DO NOT EDIT THIS:34557)
Date: Monday, April 08, 2019 9:41:25 AM

Issue ID: 34557
Short desc: 2FA - Two Factor Authentication

Last changed by	Colleen
Reported By	Colleen
Reported On	2019-03-19 8:45 AM
Tags	
Project	ElectioNet - NH
Organization	New Hampshire
Category	
Priority	High
Assigned	Keval
Status	New
ConvBgId	

comment 360635 posted by Colleen on 2019-04-08 9:40 AM, 0 seconds ago

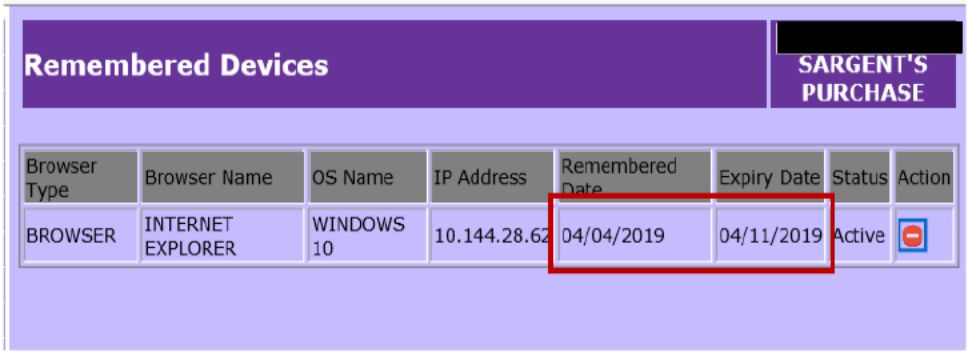
The one day remembering of the device was tested and it passed.

Last week on 04/04/2019, I set the settings for 7 days to remember the device.

It states my "Expiry Date" is 04/11/2019.

I was forced to log in with a code this morning. Today is 04/08/2019.

Could you look into this for me?



changed by Colleen on 2019-04-08 9:40 AM, 0 seconds ago

changed module number from "" to "2FA - Two Factor Authentication - Remembered Devices"

comment 359673 posted by Colleen on 2019-03-21 8:50 AM, 18 days ago

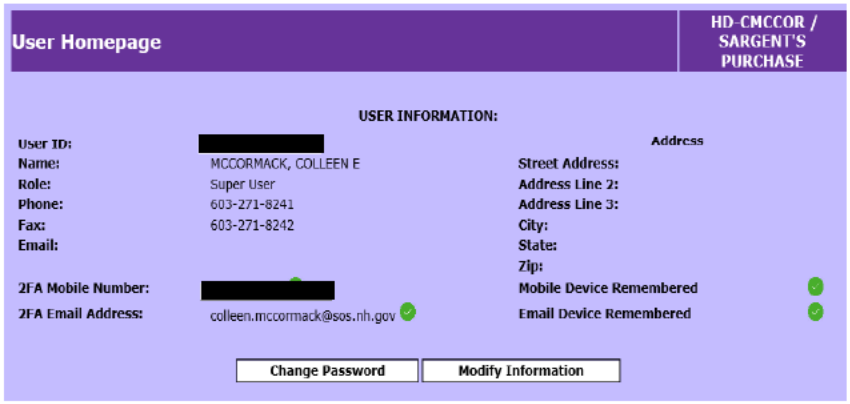
This did not pass. My rememebered device expired today and I was able to log into UAT without any prompt for a code.

changed by Colleen on 2019-03-21 8:50 AM, 18 days ago

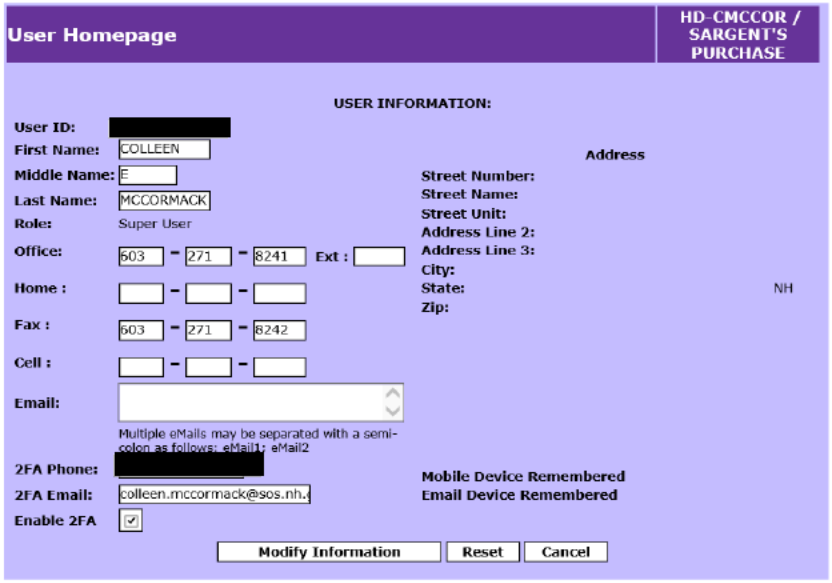
changed module number from "" to "2FA - Two Factor Authentication - Remembered Devices"

comment 359562 posted by Colleen on 2019-03-19 10:08 AM, 19 days ago

I have investigated further and on "My information" screen for the user it still has 2 green check boxes next to Mobile and Email Device Remembered.



On the "User Homepage" where the state enters the information, there are no green check marks, but there is also no text saying "Not Verified"



changed by Colleen on 2019-03-19 10:08 AM, 19 days ago

changed module number from "" to "2FA - Two Factor Authentication - Remembered Devices"

comment 359560 posted by Colleen on 2019-03-19 8:45 AM, 20 days ago

Bhanu,

I set the 2FA to expire the remembered devices for one day. Today is the day it expired. I had it remember my device. Today when I logged into UAT, I went right to the System Reminders screen.

It did not ask me to authenticate or ask me for code. I had done this test once before and I had the same results.

I then went to System -> Maintain TFA -> TFA Settings, I clicked on "Reset" system statewide. This fixed the issue.

ISSUE: I will not know when anyone's remebered device expires. The system should automatically ask them for a code once again and to "Authenticate &

remember the device."

I have reset the Remembered device for 7 days.

From:	devcenter@pcctg.com
To:	Colleen McCormack
Subject:	Issue:34964 of ElectioNet - NH project and New Hampshire organization was updated - Password Updates (DO NOT EDIT THIS:34964)
Date:	Monday, June 03, 2019 1:27:07 PM

Issue ID: 34964
Short desc: Password Updates

Last changed by	bpothugunta
Reported By	Colleen
Reported On	2019-06-03 12:17 PM
Tags	
Project	ElectioNet - NH
Organization	New Hampshire
Category	
Priority	
Assigned	Keval
Status	New
ConvBgId	

comment 363861 posted by bpothugunta on 2019-06-03 12:53 PM, 1 seconds ago

Colleen,

We will work on this and update you. Thank You.

changed by bpothugunta on 2019-06-03 12:53 PM, 1 seconds ago

changed module number from "" to "NH SOS 201"

changed by bpothugunta on 2019-06-03 12:53 PM, 1 seconds ago

changed module number from "" to "System -> My Information - Change Password"

file 363844 attached by Colleen on 2019-06-03 12:18 PM, 35 minutes ago

Password Updates

attachment: NH SOS 201 - Password Update 2019.doc

size: 340480 content-type: application/msword

comment 363843 posted by Colleen on 2019-06-03 12:17 PM, 36 minutes ago

Update the length of the characters of the password and make it a hard warning to change your password, when the password has expired.

See attached document.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

Why should State and Local Election Officials be interested in MFA?

Implementing MFA makes it more difficult for an adversary to gain access to secure databases, applications, and other election infrastructure assets. MFA can help prevent adversaries from gaining access to your organization's assets even if passwords are compromised through phishing attacks or other means.

Increasingly, a user ID and password combination alone does not provide enough protection against unauthorized login. One of the major drawbacks of using an ID and password system alone is the requirement to maintain a password database. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. These factors reduce the security of password protected systems and resources more each day.

How does MFA work?

MFA requires system or network users to present two or more credentials at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- **Something you know:** like a password, Personal Identification Number (PIN), or answers to security questions;
- **Something you have:** like a smart card, mobile token, or hardware token; and
- **Some form of biometric factor** (e.g., fingerprint, voice recognition).

For example, MFA could require users to insert a smart card ID into a card reader (first factor) and then enter a password (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

The added security offered by MFA can simplify the user login process by using single-sign on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time.

Consider deploying an MFA capability to cover voter registration systems, election night reporting systems, or other election office IT systems. Implementation schedules and costs vary depending on the MFA solution your organization chooses and the assets that it covers. These options range from implementing a single sign-on environment to supplementing an existing password-based login system with a second authentication factor, such as a time-limited, single-use code delivered by token or through a smartphone app generator.

Public Comment of Meagan Wolfe

Interim Administrator
Wisconsin Elections Commission

U.S. Elections Assistance Commission
April 10, 2019

Version 2.0 of the Voluntary Voting System Guidelines
For Information Only: No Position Registered

Honorable Members:

Thank you Commissioners and staff of the EAC for hosting this meeting and for welcoming input from state and local election officials on the Voluntarily Voting Standards and Guidelines. Your willingness to receive input at this critical juncture is vital to the long-term success of the standards and certification process. I am Meagan Wolfe and it's my honor to serve as the Administrator for the State of Wisconsin Elections Commission and as the Chief Election Official for the State of Wisconsin. The Wisconsin Elections Commission has not taken a position on the VVSG, so I am presenting today's comments for information only.

Under the current EAC standards, voting systems cannot be updated quickly when they are patched, modernized, or otherwise changed. I urge you to consider state and local election officials' need to ensure that lack of quorum or ideological deadlock among EAC Commissioners does not affect our ability to provide our voters with modern, secure and usable voting equipment.

For many years, the Wisconsin Elections Commission and its predecessor agencies would not approve voting system that did not meet EAC certification and standards. Then, local election officials' strong desire to purchase new voting systems with modern features spurred a change in the process and ultimately the law. Local election officials experienced delays in the EAC process and found that the standards did not adequately reflect the requirements needed to ensure security in modern voting technology. Therefore, in 2015 a law was passed to eliminate the requirement that all voting systems approved for use in Wisconsin be accredited by the EAC and giving the state the ability to approve systems outside of the EAC certification process.

However, local election officials and state officials are still very hesitant to pursue equipment that has not been certified by EAC or without modern VVSG standards to guide our certification process. EAC certification and standards should be a foundation on top of which our state standards are built, not an outdated roadblock we need to circumvent.

Election technology and security are dynamic. Standards that drive the development of election technology also need to be dynamic in order to keep pace. The tools we use to protect elections today are not the same tools that will be needed to protect elections tomorrow. Standards for our voting equipment are just one of many important tools we rely on as election officials. We must ensure that the principals and guidelines in place today are flexible enough to address current and future threats

As a first step, I urge the Commission to affirmatively vote to adopt the VVSG 2.0 principles and guidelines. This will solidify a vital tool for election officials to rely on as we undertake the important work of modernizing and updating our voting systems. I further urge you to plan for and allow for quick changes that may be needed. This can be accomplished by allowing the EAC Testing and Certification staff the authority to approve the requirements and test assertions, independent of the Commission. You can also further prepare the VVSG for the future by including a mechanism for approval absent a quorum or in the case of a deadlock of the Commission.

Unfortunately, election security needs do not evolve on an ideal timeline or under ideal circumstances. Contingency planning is essential to elections. As election officials, we never want to have to use our contingencies, but we must prepare strong contingencies to ensure strong elections. The VVSG should be held to this same standard. Let's work towards building resilient standards that will support secure elections, even under less than ideal circumstances. By adopting the recommendations of the Technical Guidelines Development Committee, the Standards Board, and the Board of Advisors, the EAC helps to ensure election officials have the tools we need to address the evolving challenges we may face in a timely manner.

Thank you again for the opportunity to speak with you. I appreciate your willingness to collect feedback and work towards the development of the best possible standards to help us accomplish our shared goal of administering secure, fair, and transparent elections.

Respectfully submitted,

Meagan Wolfe
Interim Administrator
Wisconsin Elections Commission
608-266-8005 / meagan.wolfe@wi.gov

From:	Amy Cohen
To:	Amy Cohen
Subject:	Update, 3/28
Date:	Thursday, March 28, 2019 3:38:28 PM
Attachments:	Request for Applications - NGA Policy Academy on Election Cybersecurity.pdf 2019 NPF Featuring a Special Election Mail Forum.pdf FW ISAC CYBER ALERT Potentially Compromised Election Official Accounts Sending Cloud Storage Credential Harvesting Emails - TLP AMBER.msg

Good afternoon, all!

- Earlier this week, the EI-ISAC sent out an alert regarding an increase in phishing and credential harvesting attempts specifically targeting the election community. I've attached the alert they sent out as it may have gone to your spam (I removed the offending link). Please stay alert, be wary of links and attachments, and remind your locals to do the same. There is no shame in calling or emailing someone directly to confirm that they meant to send an email. **If you get a phishing email or any other suspicious email, please send it to the ISAC as an attachment:** submission@malware.cisecurity.org.
- You may have read about a supply chain vulnerability recently exposed in Asus computers. The company says it will be contacting customers impacted by the issue, but this is a good reminder to be aware of the hardware and software in use in your state and to be vigilant about updating software and installing patches.
- The NASED Summer conference is rapidly approaching! We will meet in Austin, TX, July 14-16 at the Omni Hotel, and you can click here to book your room ($146/night plus taxes and fees). Registration will open in a week or two, but book your rooms early before I open the block to the masses. There will be a GCC meeting on Saturday, July 13.
- Speaking of Austin, the NASED Board is meeting this weekend to discuss, among other things, the summer conference agenda. If you have ideas for things you'd like to see on the agenda, please send them to me or to your regional rep.
- The EAC released their 2018 report to Congress.
- Non Profit Vote and the US Election Project released a report on turnout in the 2018 election, called "America Goes to the Polls." Congratulations Minnesota!
- A reminder about the National Governor's Association application for its Policy Academy on Election Cybersecurity (attached). This has also been sent to NASS and to NGA members, so you are likely going to see it from many sides. The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364) or David Forscey (dforscey@nga.org; 202-624-5356). Applications are due by **8pm ET on May 10, 2019**. Both NASS and NASED worked with NGA on the RFA itself and are helping to make sure this project is valuable for state election offices.
- Don't forget about the opportunity to weigh in on the VVSG. Comments must be received by 4pm ET on May 29, 2019 and can be submitted to votingsystemguidelines@eac.gov. The notice indicates that the 2.0 document is available on the EAC website, and here is the link. If you have questions or want to better understand what's going on, feel free to reach out.

- Upcoming Events:
    - The National Postal Forum will host a special "Election Mail" forum at this year's National Postal Forum on Monday, May 6 in Indianapolis, IN. Come hear top election officials discuss topics such as; Addressing: NCOA & ACS for better voter rolls, Design: Ballot envelopes & postcard applications, Tracking: Full service, STID, IMb - the new "postmark" for authentication. This will be an opportunity for you to meet/network with the VP of Product Marketing to discuss pertinent Election Mail topics during the Executive Dialogue session.

      Special Registration for this event includes: One Day Conference Registration: $99 (Monday May 6), Sunday Evening NPF Welcome Reception (May 5), Monday General Session and Luncheon, Exhibit Hall Access, and Exhibit Hall Reception. Registration information is attached. For more information, contact Dan Bentley (202 268 5705, daniel.m.bentley@usps.gov)

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Public Hearing
Date: Monday, April 08, 2019 11:37:03 AM
Attachments: NASED VVSG 2.0 Talking Points.pdf

Good morning all,

I'm looking forward to seeing many of you in Memphis later this week.

I put together some talking points summarizing NASED's position on the VVSG 2.0 for your reference. They're high level, and focus only on the proposed structure. If you are planning to participate in the public hearing – which I hope you all will – feel free to use them as much or as little as you'd like. If you are not able to attend the public hearing, you are still able to submit comments in writing for the record.

Safe travels!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: [redacted]
Follow us on Twitter @NASEDorg and on Facebook!

From:	Amy Cohen
To:	Anthony Stevens
Subject:	FW: Update, 3/28
Date:	Friday, April 26, 2019 1:27:06 PM

See below!

From: Amy Cohen <acohen@nased.org>
Date: Monday, April 1, 2019 at 3:29 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: Re: Update, 3/28

They're open to election officials, but not the general public. I don't usually advertise it, but because we're not collocated with NASS, I feel a little better about the space constraints.

You're welcome to attend, but fair warning that they are snoozy!

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Date: Monday, April 1, 2019 at 3:16 PM
To: Amy Cohen <acohen@nased.org>
Subject: RE: Update, 3/28

Amy,

Will the Saturday, July 13, GCC meeting be open to the public, or members of NASED?

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Amy Cohen <acohen@nased.org>
Sent: Thursday, March 28, 2019 3:05 PM
To: Amy Cohen <acohen@nased.org>
Subject: Update, 3/28

Good afternoon, all!

- Earlier this week, the EI-ISAC sent out an alert regarding an increase in phishing and credential harvesting attempts specifically targeting the election community. I've attached the alert

they sent out as it may have gone to your spam (I removed the offending link). Please stay alert, be wary of links and attachments, and remind your locals to do the same. There is no shame in calling or emailing someone directly to confirm that they meant to send an email. **If you get a phishing email or any other suspicious email, please send it to the ISAC as an attachment:** submission@malware.cisecurity.org.

- You may have read about a supply chain vulnerability recently exposed in Asus computers. The company says it will be contacting customers impacted by the issue, but this is a good reminder to be aware of the hardware and software in use in your state and to be vigilant about updating software and installing patches.
- The NASED Summer conference is rapidly approaching! We will meet in Austin, TX, July 14-16 at the Omni Hotel, and you can click here to book your room ($146/night plus taxes and fees). Registration will open in a week or two, but book your rooms early before I open the block to the masses. There will be a GCC meeting on Saturday, July 13.
- Speaking of Austin, the NASED Board is meeting this weekend to discuss, among other things, the summer conference agenda. If you have ideas for things you'd like to see on the agenda, please send them to me or to your regional rep.
- The EAC released their 2018 report to Congress.
- Non Profit Vote and the US Election Project released a report on turnout in the 2018 election, called "America Goes to the Polls." Congratulations Minnesota!
- A reminder about the National Governor's Association application for its Policy Academy on Election Cybersecurity (attached). This has also been sent to NASS and to NGA members, so you are likely going to see it from many sides. The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364) or David Forscey (dforscey@nga.org; 202-624-5356). Applications are due by **8pm ET on May 10, 2019**. Both NASS and NASED worked with NGA on the RFA itself and are helping to make sure this project is valuable for state election offices.
- Don't forget about the opportunity to weigh in on the VVSG. Comments must be received by 4pm ET on May 29, 2019 and can be submitted to votingsystemguidelines@eac.gov. The notice indicates that the 2.0 document is available on the EAC website, and here is the link. If you have questions or want to better understand what's going on, feel free to reach out.
- Upcoming Events:
    - The National Postal Forum will host a special "Election Mail" forum at this year's National Postal Forum on Monday, May 6 in Indianapolis, IN. Come hear top election officials discuss topics such as; Addressing: NCOA & ACS for better voter rolls, Design: Ballot envelopes & postcard applications, Tracking: Full service, STID, IMb - the new "postmark" for authentication. This will be an opportunity for you to meet/network with the VP of Product Marketing to discuss pertinent Election Mail topics during the Executive Dialogue session.

      Special Registration for this event includes: One Day Conference Registration: $99 (Monday May 6), Sunday Evening NPF Welcome Reception (May 5), Monday General Session and Luncheon, Exhibit Hall Access, and Exhibit Hall Reception. Registration

information is attached. For more information, contact Dan Bentley (202 268 5705, daniel.m.bentley@usps.gov)

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Re: Update, 3/13
Date: Wednesday, March 13, 2019 2:22:52 PM

A quick addition regarding dark web activity:

- DHS and the ISAC continue to see reports of voter registration lists available for sale on the dark web, similar to what we saw in October. Remain vigilant about monitoring your systems, and contact DHS (nccicccustomer@hq.dhs.gov) and the ISAC (soc@cisecurity.org) if you see anything anomalous.

From: Amy Cohen <acohen@nased.org>
Date: Wednesday, March 13, 2019 at 11:39 AM
To: Amy Cohen <acohen@nased.org>
Subject: Update, 3/13

Hi all,

A couple things so far this week:

- HR 1 passed the House on Friday, 234 to 193. Full text available here (it's 706 pages, so… head's up). Senate Majority Leader Mitch McConnell (R-KY) has been clear that HR 1 will not get a vote in the Senate, so this could be where the story ends, at least for now.
- Chris Krebs, Director, Cybersecurity and Infrastructure Security Agency at DHS will testify before the House Appropriations Subcommittee on Homeland Security this afternoon at 2pm ET on Securing Federal Networks and State Election Systems. Live stream it here, and his written remarks are available here.
- Last week, NASS President Jim Condos sent the attached letters, on behalf of the organization, to Twitter and Facebook regarding their use of third-party voter registration platforms and their work on misinformation. Copies were sent to the US House Committee on Administration, the US Senate Committee on Rules and Administration, the EAC, DHS, and to us.
- Reminder to nominate yourselves, your SOS or LtG, your IT staff, or your locals for leadership of the EI-ISAC. Consistent with the charter that we recently approved, the composition of the Executive Committee will be as described below. To apply, submit the name and bio (up to 250 words!) **by March 15 (this Friday!)** via this link; the membership will vote from March 25 – April 5. Responsibilities for the Executive Committee are also described at that link. If you have questions, please contact elections@cisecurity.org.
    - 6 State Election seats (half will serve 1 year terms, half will serve 2 year terms)
        - 2 SOS or Lieutenant Governors
        - 2 State Election Directors

        - 2 IT security leads from state offices
    - 7 Local Election seats
        - 5 local election officials (three will serve 2 year terms, two will serve 1 year terms)
        - 2 local election office IT representatives
- DHS provided the attached feedback form to solicit feedback on their elections work and guide future improvements. Please return the completed form to etf.feedback@rand.org. I sent this last week, and when I spoke to the evaluators yesterday, they told me they had not received any feedback. I know you all have opinions, please share them!
- Upcoming events:
    - **REMINDER:** The National Postal Forum will host a special "Election Mail" forum at this year's National Postal Forum on Monday, May 6 in Indianapolis, IN. Come hear top election officials discuss topics such as; Addressing: NCOA & ACS for better voter rolls, Design: Ballot envelopes & postcard applications, Tracking: Full service, STID, IMb - the new "postmark" for authentication. This will be an opportunity for you to meet/network with the VP of Product Marketing to discuss pertinent Election Mail topics during the Executive Dialogue session.

      Special Registration for this event includes: One Day Conference Registration: $99 (Monday May 6), Sunday Evening NPF Welcome Reception (May 5), Monday General Session and Luncheon, Exhibit Hall Access, and Exhibit Hall Reception. To register, and for a look at the draft agenda, please see the attached word document.

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

NATIONAL ASSOCIATION of
STATE ELECTION DIRECTORS

April 25, 2019

The Honorable Zoe Lofgren
Chairperson, Committee on House Administration
United States House of Representatives
1309 Longworth House Office Building
Washington, DC 20515

Dear Chairperson Lofgren:

On behalf of the National Association of State Election Directors (NASED), thank you for your letter dated April 10, 2019 inquiring about usage of the $380 million in Help America Vote Act (HAVA) funds that Congress appropriated in March 2018. The report provided to you by the U.S. Election Assistance Commission (EAC) discusses data through September 30, 2018, because that is what states were required to provide to the EAC at the end of December as part of their annual reporting. The EAC has not asked for, nor are the states required to provide, more recent data at this time.

As you requested, however, NASED forwarded your letter to our members who represent all 50 states, the District of Columbia, American Samoa, Guam, Puerto Rico, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands, the last of which, as you are aware, is not covered under HAVA despite running federal elections for delegate to Congress and participating in the presidential nomination process. In 16 states and territories, NASED members are the Chief Election Official of their jurisdiction. To facilitate responses to your request, NASED provided contact information for Tanya Sehgal, Elections Counsel for the House Committee on House Administration, so that states and territories can respond directly to her with the information you asked for.

Although the EAC disbursed funds to the states and territories quickly—all received their monies by mid-September—it was never realistic that significant percentages of those funds would be spent before the November 2018 general election. Many states require legislative approval to spend funds, development of business requirements for complex systems can take months to years to complete, state procurement requirements do not prioritize speed, and voting technology is made to order. Beyond that, state, territorial, and local election officials rightfully

1342 Florida Avenue NW
Washington, DC 20009

www.nased.org
240-801-6029

prioritized running the November 2018 general election, which we can confidently say was the most secure election in American history. We do not want a repeat of 2003, when election officials rushed to purchase new equipment upon receipt of their HAVA funds, only to learn not long after that the equipment purchased was not the best available option. Election officials want to spend their new HAVA funds responsibly, and that often takes some time.

NASED does not take a position on federal funding, so we will defer to each state or territory to answer your question about the amount of federal money they need or want. I would be remiss, however, if I did not take this opportunity to encourage Congress to consider sustained funding for elections instead of one-time hand-outs. Many of the greatest problems in our field stem from inconsistent access to the funding needed to complete necessary upgrades of voting equipment and systems, databases, websites, and more.

The EAC report on fiscal year 2018 includes details about the funds that states have left from the initial disbursement of HAVA funds in 2003. Given the uncertain funding landscape, it is no surprise that so many states have held onto that money for so long to make sure they have it in case of an emergency. NASED fully expects the states and territories to meet the timing requirements of the 2018 HAVA funding, but also understands why jurisdictions may want to make the money last as long as possible.

Thank you again for contacting NASED about this important issue. We look forward to working with you and your colleagues to maintain a secure, resilient election system that Americans can be proud of. If you or your staff have any questions, please feel free to contact Amy Cohen, Executive Director of NASED, at 240-801-6029 or acohen@nased.org.

Best,

Keith Ingram
President, National Association of State Election Directors
Director of Elections, Texas Secretary of State

From: Amy Cohen
To: Amy Cohen
Subject: Update, 3/21
Date: Thursday, March 21, 2019 11:04:20 AM
Attachments: Request for Applications - NGA Policy Academy on Election Cybersecurity.pdf
D3P DecCon AAR Report v2.0 INTERNAL[1].pdf

Good morning, all!

- The National Governor's Association has released the application for its Policy Academy on Election Cybersecurity, and it is attached. Those of you at our conference heard a bit about this, but the goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364) or David Forscey (dforscey@nga.org; 202-624-5356). Applications are due by **8pm ET on May 10, 2019**.
- Senators Van Hollen (D-MD), Collins (R-ME), Cardin (D-MD), and Rubio (R-FL) introduced the Protect our Elections Act late last week. The bill requires, among other things:
    - The EAC and DHS to release cybersecurity best practices for vendors; and,
    - The EAC create and maintain a database of qualified election service providers
        - A qualified election service provider is under US ownership and control (created or organized in a country that is a member of the Five Eyes Alliance), agrees to meet and maintain its infrastructure under the previously mentioned cybersecurity best practices, and agrees to report any known or suspected incident to the relevant state election official, the EAC, and DHS.
- The ISAC extended the deadline for nominations to the EI-ISAC Executive Committee because they didn't get enough submissions. **The deadline is now tomorrow, March 22**. I spoke with Ben Spear last week regarding the time commitment: they estimate one hour per month, plus attendance at the annual meeting. We need a diverse group of SOS's/LtG's, Election Directors, State IT staff, local election officials, and local election office IT staff to represent all of the diversity in election administration: township/county, top-down/bottom-up, SOS/Board, etc. Consistent with the charter that we recently approved, the composition of the Executive Committee is described below. To apply, submit the name and bio (up to 250 words!) via this link. Responsibilities for the Executive Committee are also described at that link. If you have questions, please contact elections@cisecurity.org.
    - 6 State Election seats (half will serve 1 year terms, half will serve 2 year terms)
        - 2 SOS or Lieutenant Governors
        - 2 State Election Directors
        - 2 IT security leads from state offices
    - 7 Local Election seats
        - 5 local election officials (three will serve 2 year terms, two will serve 1 year terms)
        - 2 local election office IT representatives
- Based on feedback from their meeting in December, the Belfer Center put together the attached After Action Report summarizing the successes of the 2018 election and areas where

we can still make progress.

- You probably heard last week that the Defense Department's Defense Advance Research Projects Agency (DARPA) will be working with Galois over the next year to build an open source ballot marking device and optical scan voting system. They're planning to bring the ballot marking device to Def Con in October of this year. DARPA (the inventors of the internet) has committed $10 million to this effort. More to come on this, I'm sure.

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 3/5
Date: Tuesday, March 05, 2019 4:59:09 PM
Attachments: ETF_2018_feedback[1].pdf
WG Rosters (Jt and GCC)[1].xlsx

Hello all, and happy March!

- The House Rules Committee meets at 5pm ET today to determine the rules for HR 1 when it goes to the House floor, possibly as soon as this week.
- In other HR 1 news, the Congressional Budget Office released their estimate of the bill's cost on Friday, March 1. According to their review, the total cost for the bill is between $2.4 billion and $2.5 billion for FYs 2019 - 2024, with $1.4 - $1.5 billion in voting system grants in that time and $750 million in EAC grants in that time. Note that HR 1 authorizes the money (says what could be spent and how) but does not actually appropriate the money (put money in pockets). Appropriations come in a different bill later this year.
- Attached is a list of the rosters for the current GCC Working Groups and joint GCC/SCC Working Groups, along with descriptions of the working groups. This is a great opportunity for you, as well as for your colleagues and staff in your offices who have expertise or interests but don't get to participate as much at the national level. **If you're on a working group and don't want to be, or if you want to be on a working group, please let me know by end of day Friday**. If you thought you were on one and aren't on the list, let me know that, too – rosters are tough to keep current.
- The EI-ISAC sent out a call for nominations to the EI-ISAC Executive Committee earlier this week. Consistent with the charter that we recently approved, the composition of the Executive Committee will be as described below. To apply, submit the name and bio (up to 250 words!) by March 15 via this link; the membership will vote from March 25 – April 5. Responsibilities for the Executive Committee are also described at that link. If you have questions, please contact elections@cisecurity.org. I hope many of you will consider running and will nominate members of your IT staff!
    - 6 State Election seats (half will serve 1 year terms, half will serve 2 year terms)
        - 2 SOS or Lieutenant Governors
        - 2 State Election Directors
        - 2 IT security leads from state offices
    - 7 Local Election seats
        - 5 local election officials (three will serve 2 year terms, two will serve 1 year terms)
        - 2 local election office IT representatives
- DHS provided the attached feedback form to solicit feedback on their elections work and guide future improvements. Please return the completed form to etf.feedback@rand.org. Matt assures me this is not a bureaucratic exercise and that your feedback will be incorporated into their work.
- Upcoming events:

- The National Postal Forum will host a special "Election Mail" forum at this year's National Postal Forum on Monday, May 6 in Indianapolis, IN. Come hear top election officials discuss topics such as; Addressing: NCOA & ACS for better voter rolls, Design: Ballot envelopes & postcard applications, Tracking: Full service, STID, IMb - the new "postmark" for authentication. This will be an opportunity for you to meet/network with the VP of Product Marketing to discuss pertinent Election Mail topics during the Executive Dialogue session.

  Special Registration for this event includes: One Day Conference Registration: $99 (Monday May 6), Sunday Evening NPF Welcome Reception (May 5), Monday General Session and Luncheon, Exhibit Hall Access, and Exhibit Hall Reception. For more information, contact Dan Bentley (202 268 5705, daniel.m.bentley@usps.gov)

- **REMINDER**: Those of you at our conference last month heard from David Forscey at the National Governors Association (NGA) about some of their growing work in elections. There will be more information on their elections project coming soon, but NGA will also be hosting a National Summit on State Cybersecurity in Shreveport, LA, May 14-15. There will definitely be an elections component, as well as other topics that could be of value to NASED members. If you or someone in your office is interested in attending, let me know; they're able to offer a handful of comped registrations to us (you still cover travel and lodging).

- I wrote a lot about the VVSG 2.0 public comment last week, so I won't repeat myself except to say: don't forget about the opportunity to weigh in. Comments must be received by 4pm ET on May 29, 2019 and can be submitted to votingsystemguidelines@eac.gov. The notice indicates that the 2.0 document is available on the EAC website, and here is the link. If you have questions or want to better understand what's going on, feel free to reach out. (Get used to seeing this blurb at the end of my update emails!)

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/1
Date: Wednesday, May 01, 2019 9:21:02 AM
Attachments: RFA - Policy Academy on Election Security v3.docx
Draft Member Agenda_05.01.19.pdf

Good morning all, and Happy May Day (and Lei Day in Hawaii)!

- The House Oversight Committee will hold a hearing at 2pm ET today called "Protecting the Right to Vote: Best and Worst Practices." Witnesses are listed below. They are looking through a lens of enfranchisement, but it also sounds like this will be a very broad hearing and will tie back to HR 1.
    - **Ms. Leigh Chapman,** Director, Voting Rights Program, The Leadership Conference on Civil and Human Rights
    - **Mr. Dale Ho,** Director, Voting Rights Project, American Civil Liberties Union
    - **Ms. Myrna Perez,** Deputy Director, Democracy Program, Brennan Center for Justice
- The Center for Internet Security released their procurement guide yesterday, called "A Guide for Ensuring Security in Election Technology Procurements." Many state and local election officials and election technologists provided feedback on this document, so it is truly an election-specific guide. Among other things, this document provides best practices for procurement in a very practical way, including suggested language for RFPs/RFIs/what-have-you, what would constitute good and bad responses, and additional context or information to help you understand that practice or concept. If you don't want to read 65 pages, they also break it down by section here.
- And now for the moment you've all been waiting for…attached is a draft agenda for our upcoming Summer Conference in Austin, July 14-16 (don't forget to register!). I'm in the process of inviting people, futzing around with the times to include everything we want to, and planning fun, and will be sure to share updates regularly. Please let me know if you have any questions.
- NASED is working with NASS on a working group of communications directors and social media companies to provide feedback on misinformation efforts, community standards, and similar issues. NASS put out the call to their 40 state communication directors, and I have been in touch with the NASED communications directors. The plan is to try to meet by phone quarterly, and I will keep you posted on outcomes.
- Last week, the EAC Board of Advisors met in Salt Lake City. The Board passed a resolution, similar to the recommendation passed by the EAC Standards Board, stating that the VVSG is a standalone document required by HAVA and the Requirements and Test Assertions are established by policy. Further, the resolution recommends that the EAC adopt a policy to ensure that the Requirements and Test Assertions can be updated in the absence of a quorum of EAC commissioners, provided this is deemed legal and there are clear guidelines establishing the level of authority of the staff. Because this was a resolution, it should be on the EAC Board of Advisors website, but it's not there just yet.
    - If you missed either of the public hearings that took place in conjunction with the Standards Board of Board of Advisors, here are the videos: Memphis and Salt Lake City.
- Now that it's May, another reminder about the National Governor's Association

application for its Policy Academy on Election Cybersecurity (attached). The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364). **Applications are due by 8pm ET on May 10, 2019.** Both NASS and NASED worked with NGA on the RFA itself and are helping to make sure this project is valuable for state election offices.

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

Background

- Election Directors serve on the Technical Guidelines Development Committee (TGDC), the Election Assistance Commission's (EAC) Board of Advisors, and the EAC Standards Board; NASED had a VVSG Committee when there was no quorum at the EAC to discuss solutions for how to move the standards development process forward without the EAC.
- The current voting system standards predate the first iPhone – VVSG 1.0 is from 2005 and the first iPhone came out in 2007. VVSG 1.1 made minor modifications to VVSG 1.0.
- The TGDC, the EAC Standards Board, and the EAC Board of Advisors, all of which include diverse state and local election officials and representatives from the EAC itself, voted in favor of the proposed structure of the VVSG 2.0 in September 2017 and April 2018, respectively.

Proposed Structure

- Any new standards must be flexible and adaptable to accommodate the next innovation and our changing digital world.
- NASED strongly supports the proposed structure of the VVSG 2.0, with the broad, high-level Principals and Guidelines requiring EAC Commissioner approval, and the technical requirements and test assertions being updated regularly by qualified EAC technical staff. This will allow the standards to evolve even if the agency doesn't have a quorum in the future.
- Concerns about lack of a quorum are real: as of April 10, 2019, the EAC has been without a quorum for 2,105 days, or 37.6 percent of the agency's entire existence, including during the 2012 presidential election and the 2014 and 2018 midterm elections.
- The integrity of American voting systems cannot be held hostage by lack of a quorum or philosophical differences among the commissioners.
- The entire process for development of VVSG 2.0 has been public: TGDC meetings are public, and the working groups focused on the requirements development, also public, include dozens of current and former state and local election officials from jurisdictions across the country, as well as voting system vendors, advocates, and others.
- The EAC commissioners did not vote on the current test assertions and have never voted on the test assertions. Non-technical experts should not vote on highly technical procedures.
- The proposed structure will allow the testing and certification processes to be more efficient and will permit new methods for certifying modifications, upgrades, and patches, all of which will allow election officials to better ensure the security and integrity of their voting equipment.
- It is state and local election officials, not the EAC or EAC commissioners, who bear the brunt of public ire and media hostility when voting systems are out-of-date; the election administration community needs the VVSG 2.0 to pass, and needs it to pass in the proposed flexible form.

NATIONAL ASSOCIATION of STATE ELECTION DIRECTORS

Thank you for the chance to provide feedback on Version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0). The VVSG 2.0 represents an important opportunity to advance modern voting system standards that election vendors can use to build secure, trustworthy voting technology that voters can have confidence in.

The National Association of State Election Directors (NASED) represents all 50 states, the District of Columbia, and the five U.S. territories: American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands. Our members serve on the Technical Guidelines Development Committee (TGDC), the Election Assistance Commission's (EAC) Board of Advisors, and the EAC Standards Board; NASED itself had a VVSG Committee when there was no quorum at the EAC to discuss solutions for moving the standards development process forward without the EAC.

The EAC has asked for feedback from the community on both the content of the VVSG 2.0 and the proposed structure. VVSG 1.0 was approved by the EAC in December 2005; in 2007, an effort to make significant changes to the VVSG and move to version 2.0 failed because the commissioners could not agree. In 2015, the commissioners approved minor modifications to version 1.0, updating the standard to version 1.1[1]. To put this in perspective, Apple released the first iPhone in June 2007; the current voting system standards are so technologically dated, they predate the first iPhone because the EAC commissioners could not agree on more significant revisions.

Standards must fit the world that we live in, and this requires the ability to change and adapt quickly. The proposed structure makes the Principles and Guidelines the VVSG 2.0 and leaves the technical requirements and voting system test lab test assertions separate, and therefore not in need of a vote by EAC commissioners; these additional documents would be updated consistent with a policy which would be voted on by EAC commissioners. The TGDC, the EAC Standards Board, and the EAC Board of Advisors, all of which include diverse state and local election officials and non-voting representatives from the EAC itself, voted in favor of the proposed

[1] In software development, major changes result in a change to the first digit and minor changes result in a change to the second digit; thus VVSG v.1.1 represents minor changes to VVSG v. 1.0.

1342 Florida Avenue NW
Washington, DC 20009

www.nased.org
240-801-6029

structure of the VVSG 2.0 in September 2017 and April 2018, respectively. Both the TGDC and the Board of Advisors also include technology and accessibility experts in addition to state and local election officials.

At the 2018 EAC Standards Board meeting, however, the EAC offered that EAC commissioners should not only vote on the Principles and Guidelines but on the requirements and the voting system test lab test assertions as well. This was a surprise, and defeats the purpose of designing the VVSG 2.0 as a separate document from the requirements and test assertions. Based on questioning at the Public Hearings on the VVSG 2.0 on April 10 and April 23, 2019, it is clear that the EAC commissioners continue to think this is the appropriate course of action; NASED disagrees. EAC commissioners have never cast a vote on voting system test lab test assertions.

NASED strongly supports the proposed structure of the VVSG 2.0 out for public comment, with the broad, high-level Principles and Guidelines requiring EAC commissioner approval and allowing the technical requirements and voting system test lab test assertions to be updated regularly by qualified EAC technical staff in close consultation with other experts, including those from the National Institute of Standards and Technology (NIST). This proposed structure will allow the testing and certification processes to be more efficient and permit new methods for certifying modifications, upgrades, and patches, all of which will allow election officials to better ensure the security and integrity of their voting equipment.

Consistent with the recent unanimous recommendation of the EAC Standards Board and the resolution passed by the EAC Board of Advisors, NASED views the Principles and Guidelines as the VVSG 2.0, required by the Help America Vote Act of 2002 (HAVA) and subject to EAC commissioner vote. Prior to adopting the VVSG 2.0, however, the EAC must also adopt policies governing the VVSG 2.0 that clearly state that the requirements and voting system test assertions are independent documents that do not require commissioner vote. This will allow the requirements and test assertions to be dynamic over time, even when there is no quorum of commissioners at the EAC.

EAC commissioners voting on requirements and test assertions is problematic for several reasons:

- The EAC is often without a quorum. If the requirements and test assertions are considered part of the VVSG 2.0, they cannot be updated in the absence of a quorum.

  NASED's concerns about a quorum at the EAC are not unjustified; in fact, the agency was without a quorum almost as soon as it was voted into existence. The EAC should have had a quorum within 120 days of the date of HAVA's enactment, or by February 23, 2003; the initial commissioners, however, were not appointed until December 13, 2003.[2] The EAC had a quorum from that date until December 10, 2010[3], when Commissioner Gracia Hillman left the agency. The EAC went without a quorum again until January 13, 2015,[4] and for another 317 days in 2018 and 2019 during which time Microsoft alone issued a dozen critical patches for its products.[5] In total, the EAC has been without a quorum for 2,105 days[6], or 35.6 percent of the agency's entire existence.

- The structure of the EAC – two Republican-appointed commissioners and two Democratic-appointed commissioners – makes the agency susceptible to politics. Voting system standards are not political or partisan, and cannot be hamstrung by a deadlock among the commissioners, particularly given that the commissioners typically are not technical experts. The development of the VVSG 2.0 has been a bipartisan, collaborative process from the very start, and the TGDC, Standards Board, and Board of Advisors are all bipartisan.

---

[2] Testimony of the EAC Commissioners before the U.S. House of Representatives Committee on House Administration, June 17, 2004. See page 1.

[3] Amended Notice: Request for Substantive Comments on the EAC's Proposed Requirements for Version 1.1 of the Voluntary Voting System Guidelines (VVSG), published in the Federal Register October 1, 2012.

[4] EAC Major Management and Performance Challenges report, submitted to EAC Acting Executive Director Alice Miller by EAC Acting Deputy Inspector General Roger LaRouche, October 13, 2015. See page 3.

[5] Data on critical patches courtesy of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

[6] February 23, 2003 to December 13, 2003 is 293 days; December 10, 2010 to January 13, 2015 is 1,495 days; March 24, 2018 to February 4, 2019 is 317 days. As of May 2, 2019, the EAC has been in existence for 5,912 days.

- Technical standards must be reviewed and approved by technical experts, not political appointees. At the EAC, the appropriate approver for technical standards is the Director and staff in the Testing and Certification department of the agency, in consultation with NIST and others, similar to how the EAC Executive Director and Director of Testing and Certification are responsible for the certification of voting systems. The commissioners must trust their staff and technical experts.

- The EAC commissioners have never voted on voting system test lab test assertions. The commissioners should not vote on more than they already do: VVSG 1.0 predates the iPhone because the commissioners could not agree on more significant changes to the standards.

  Test assertions represent the process by which the test labs will achieve the requirements, and therefore they must be modified on an ongoing basis to make sure that they continue to adequately test the requirements. The EAC did not vote on the current test assertions and has never voted on them in the past; some of the current test assertions were developed by the EAC and NIST and the rest are, according to EAC staff at the 2018 Standards Board meeting, "proprietary to each of the labs."[7] While we appreciate efforts to standardize the test assertions across voting system test labs, NASED does not believe that it is appropriate for non-technical experts to vote on highly technical procedures. The test assertions should be maintained via a public process and reviewed and approved by EAC technical staff in consultation with NIST.

The proposed VVSG has been formally in development since 2015, though NASED members began discussing this proposed structure as early as 2013 on the NASED VVSG Committee. Over the last four years, technology and accessibility experts, voting system vendors, and federal experts, including representatives from NIST and the EAC itself, have contributed to the Principles and Guidelines as well as to the development of the requirements and test assertions. TGDC meetings are public, and the working groups focused on the requirements' development, also public, include dozens of current and former state and local election officials from jurisdictions across the country, as well as voting system vendors, advocates, and others. The time to raise concerns about taking the requirements out of the VVSG was when the new structure was first proposed. Now that we are so close to the finish line, and now that the security threats we face demand it more than ever, we cannot begin the standards development process again from scratch.

[7] Transcript of the 2018 EAC Standards Board Meeting, April 19-20, 2018 in Coral Gables, Florida. See pages 208 and 223.

State and local election officials, not the EAC or EAC commissioners, bear the brunt of public ire and media hostility when voting systems are out-of-date; the election administration community needs the VVSG 2.0 to pass in the proposed flexible form. The Principles and Guidelines independent from the requirements and test assertions are what the election administration community wants, and more importantly, what it needs to meet modern security standards and maintain voter confidence in our election process. It is critical that there be a mechanism for updating the technical requirements and test assertions for voting systems that does not require EAC commissioner approval. The integrity of American voting systems cannot be held hostage by lack of a quorum or philosophical differences among the commissioners. There is too much at stake.

Keith Ingram, President, NASED
Lori Augino, Incoming President, NASED
Michelle Tassinari, Vice President, NASED
Steve Trout, Treasurer, NASED
Sally Williams, Secretary, NASED
Rob Rock, Northeast Regional Representative, NASED
Jared Dearing, South Regional Representative, NASED
Meagan Wolfe, Midwest Regional Representative, NASED
Wayne Thorley, West Regional Representative, NASED
Robert F. Giles, Immediate Past President, NASED
Judd Choate, NASED
Linda Lamone, NASED

From:	Maria Benson
To:	Maria Benson
Cc:	Reynolds, Leslie; Dodd, Stacy; Milhofer, John; Lindsey Forson
Subject:	NASS Communications: 2016 Foreign Election Targeting--FW: The Cybersecurity 202: Companies are trying to crack down on shady apps that spy on partners, exes
Date:	Thursday, April 11, 2019 2:02:41 PM
Attachments:	image001.gif image002.gif

Good Afternoon Communications Directors,

The *Washington Post* cybersecurity newsletter (the PWNED section below) mentions the intelligence community has made the assessment that malicious Russian-linked actors likely targeted all 50 states' election networks in 2016, instead of the original 21 identified. **This is not new information**, as the Department of Homeland Security (DHS) has been saying this was likely for quite some time. Former DHS Secretary Nielsen also said this at the 2018 NASS Summer Conference during her keynote speech.

-

In addition, NASS has been consistently saying all 50 states consider themselves a target and states have acted accordingly to further secure and protect their election networks and systems.

You may get press inquiries on this, but keep in mind this latest intelligence assessment does not change the original conclusions that 1) only one state's voter registration database was partially breached, which changed no voter information and did not result in problems voting; and 2) no votes were changed in the 2016 election.

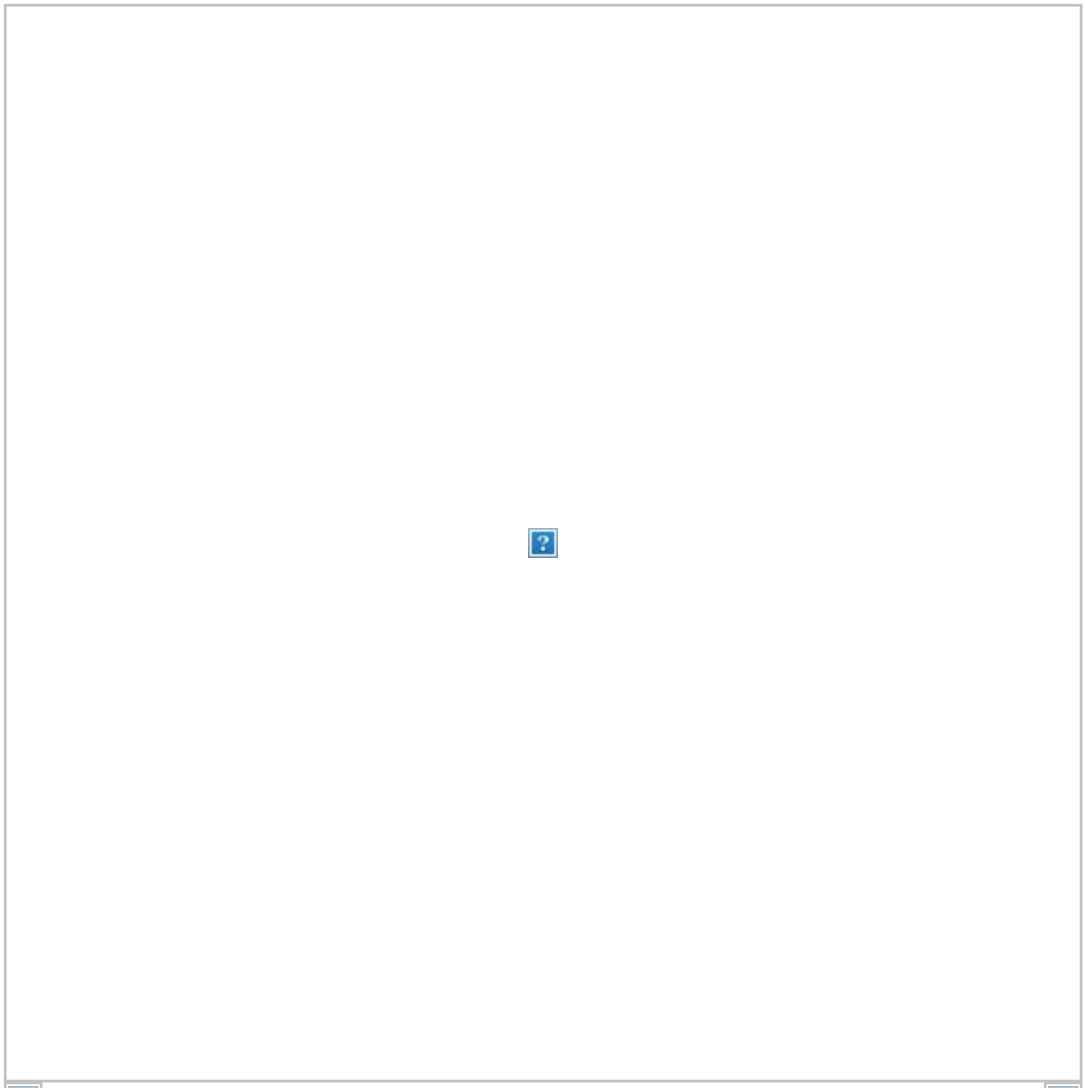
Best,

Maria (Dill) Benson
Director of Communications
National Association of Secretaries of State (NASS)
444 N. Capitol Street NW, Suite 401 | Washington, DC 20001
Desk: 202-624-3528| Cell: 423-504-1351
www.nass.org

From: The Washington Post <email@washingtonpost.com>
Sent: Thursday, April 11, 2019 12:58 PM
To: Maria Benson <mbenson@sso.org>
Subject: The Cybersecurity 202: Companies are trying to crack down on shady apps that spy on partners, exes

The Washington Post

VIEW ON WEB >



Decoding cybersecurity news in one morning tipsheet. Not on the list? Sign up here.

The Cybersecurity 202

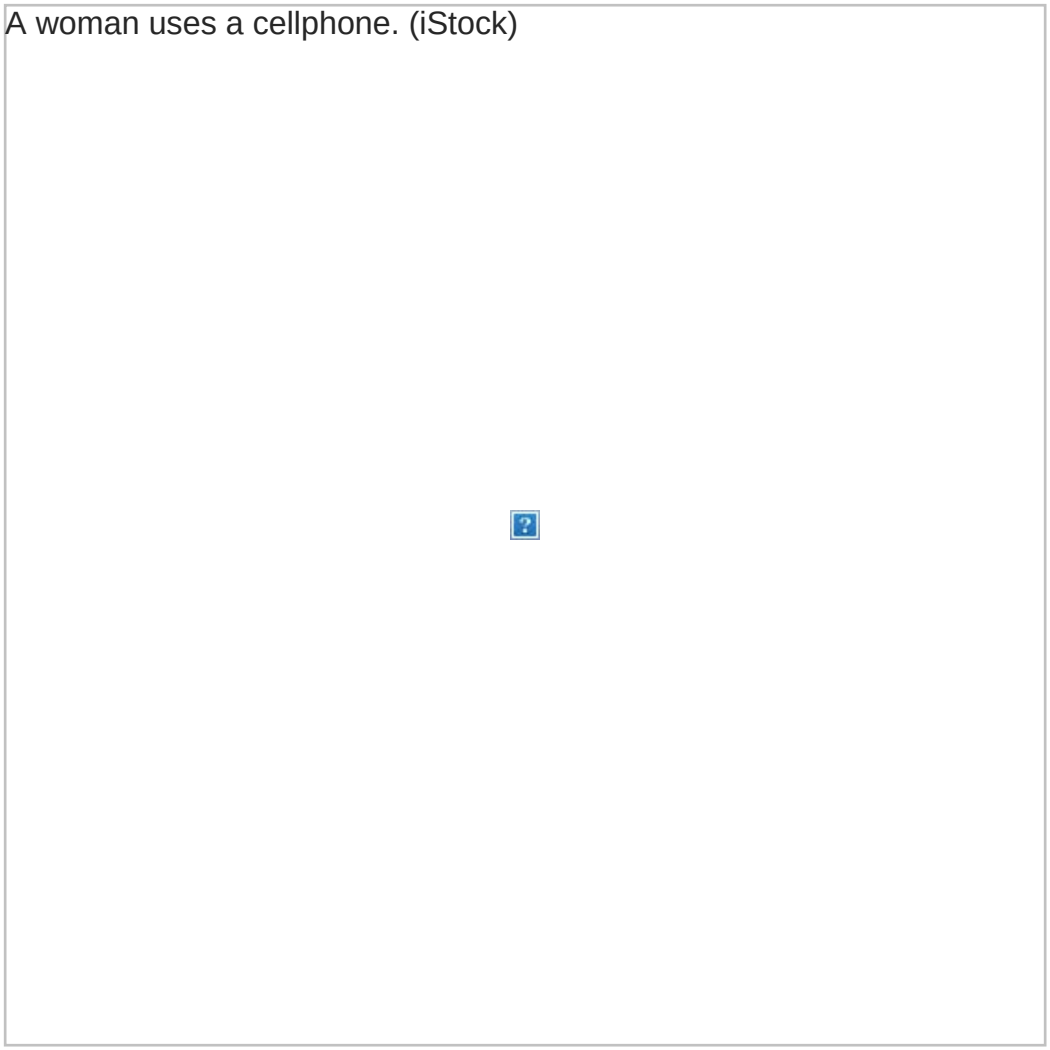
Hack your day

Share Share Tips/Feedback

Companies are trying to crack down on shady apps that spy on partners, exes

BY JOSEPH MARKS

THE KEY



A woman uses a cellphone. (iStock)

Cybersecurity companies are pledging to help customers scrub “stalkerware” apps hidden in their phones after a digital activist raised an alarm about the tools some people use to spy on partners and exes.

Symantec and McAfee both told me Wednesday that they’re trying to alert customers about these apps — also known as “commercial spyware” or “surveillanceware.”

And Russian anti-virus company Kaspersky Lab also pledged last week to start sending users special alerts when stalkerware apps are detected on their customers’ Android smartphones, and the U.S. company Lookout explained Tuesday how it offers similar protections.

The responses come after Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation, drew attention to the issue in a speech at Kaspersky's Security Analyst Summit in Singapore.

"Full access to someone's phone is essentially full access to someone's mind," Galperin told Wired before her speech. "The people who end up with this software on their phones can become victims of physical abuse, of physical stalking. They get beaten. They can be killed. Their children can be kidnapped. It's the small end of a very large, terrifying wedge."

Galperin also wants Apple, which doesn't allow external anti-virus companies to operate in its iPhones, to include better protections against stalkerware — and state and federal officials to crack down on companies that sell stalkerware, per Wired.

The responses from the cybersecurity companies that they're working on the issue shows they're taking the problem seriously — but also demonstrate how difficult it is to combat stalkerware apps, which are often tough to distinguish from apps with legitimate purposes.

There are legitimate apps, for example, that help parents monitor their children's smartphone activity or let employers ensure their workers aren't using company smartphones inappropriately, Kristy Edwards, Lookout's security intelligence director, told me.

But those apps can also be used inappropriately by people spying on spouses or exes, Edwards said. And some apps that market themselves as being for legitimate purposes are used for nefarious purposes more often than not, she said.

"A false positive is not a good thing here," Edwards told me. "You don't want to falsely accuse an app of being surveillanceware, but, on the other hand, you don't want to miss it. **It takes money and research and**

a focus on the problem for the industry to get this right."

In Lookout's case, the company typically uses artificial intelligence algorithms to find apps that might have been marketed as legitimate but are acting like malware — for example, running when the user hasn't opened them or hiding their icon.

The algorithm then sends information about those apps to researchers who investigate further and, ultimately, have to make a judgment call, Edwards said.

"There's a nuance to this that makes it really hard to fight," she said.

Many security companies have been alerting users about possible stalkerware for the past several years but lumping them into the same category as adware — software that automatically displays advertisements — and other software that is questionable or undesirable but not necessarily malicious, Kaspersky Lab security researcher Alexey Firsh told me.

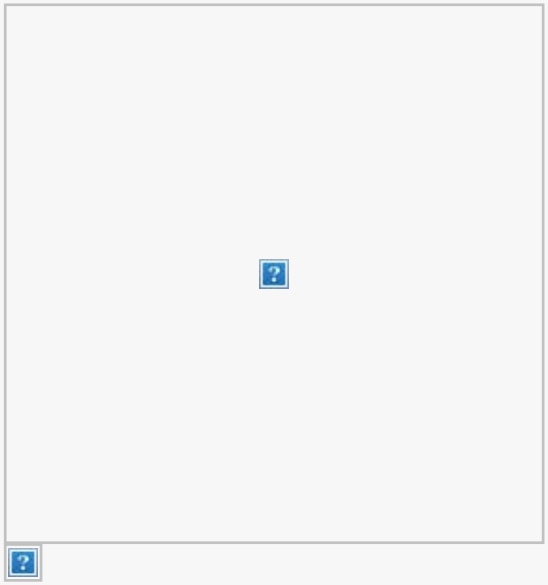
Kaspersky labeled that category "not-a-virus," but now believes that term wasn't sufficient to draw people's attention, he said. **The company is replacing it with a broader privacy alert that explains the app could be used to "compromise your personal data" including by eavesdropping on calls and reading emails and text messages.**

"We are confident that being more vocal and more proactive about this type of threat can make a big change,**"** Firsh told me. "We hope it rings a bell for an average user, so he or she will be informed about a potential threat."

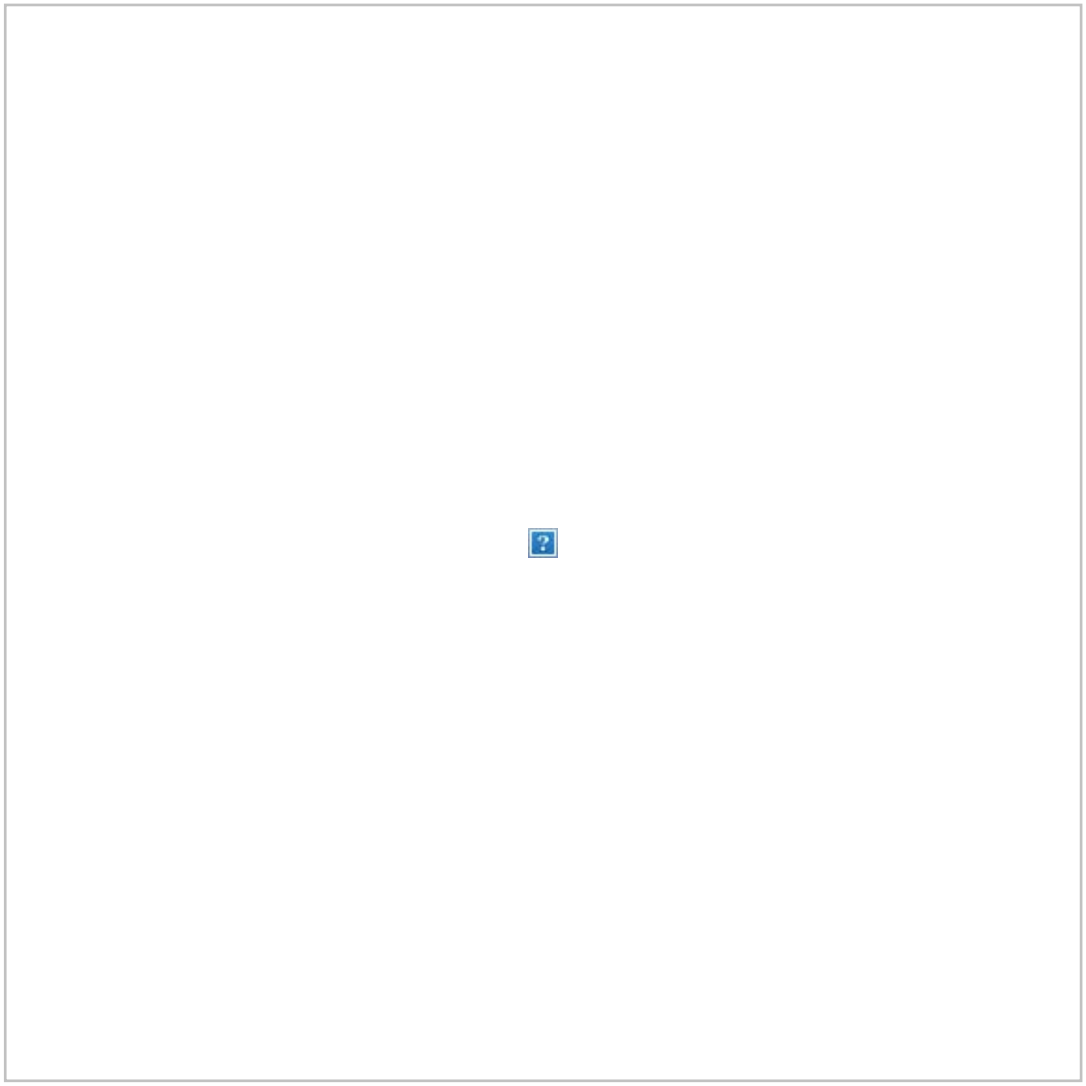
Yet to effectively combat stalkerware, companies will also have to go beyond simply alerting about it — and customers will have to be proactive about defending themselves, McAfee's mobile security research team told me in a statement.

That includes restricting all apps from accessing information they don't need and encrypting sensitive personal information such as photos, the team said.

"As is the case with so many of the threats we see, detecting and removing the known threats is just one capability," McAfee said. "You need to protect access to a device, and the data on the device. Then you need to proactively help the user by proactively crippling suspicious threats. Given the seriousness of the cyberstalker threat, you need more than one solution to address it."



PINGED, PATCHED, PWNED



WikiLeaks founder Julian Assange looks out from the balcony of the Ecuadorian embassy. (AP Photo/Matt Dunham, File)

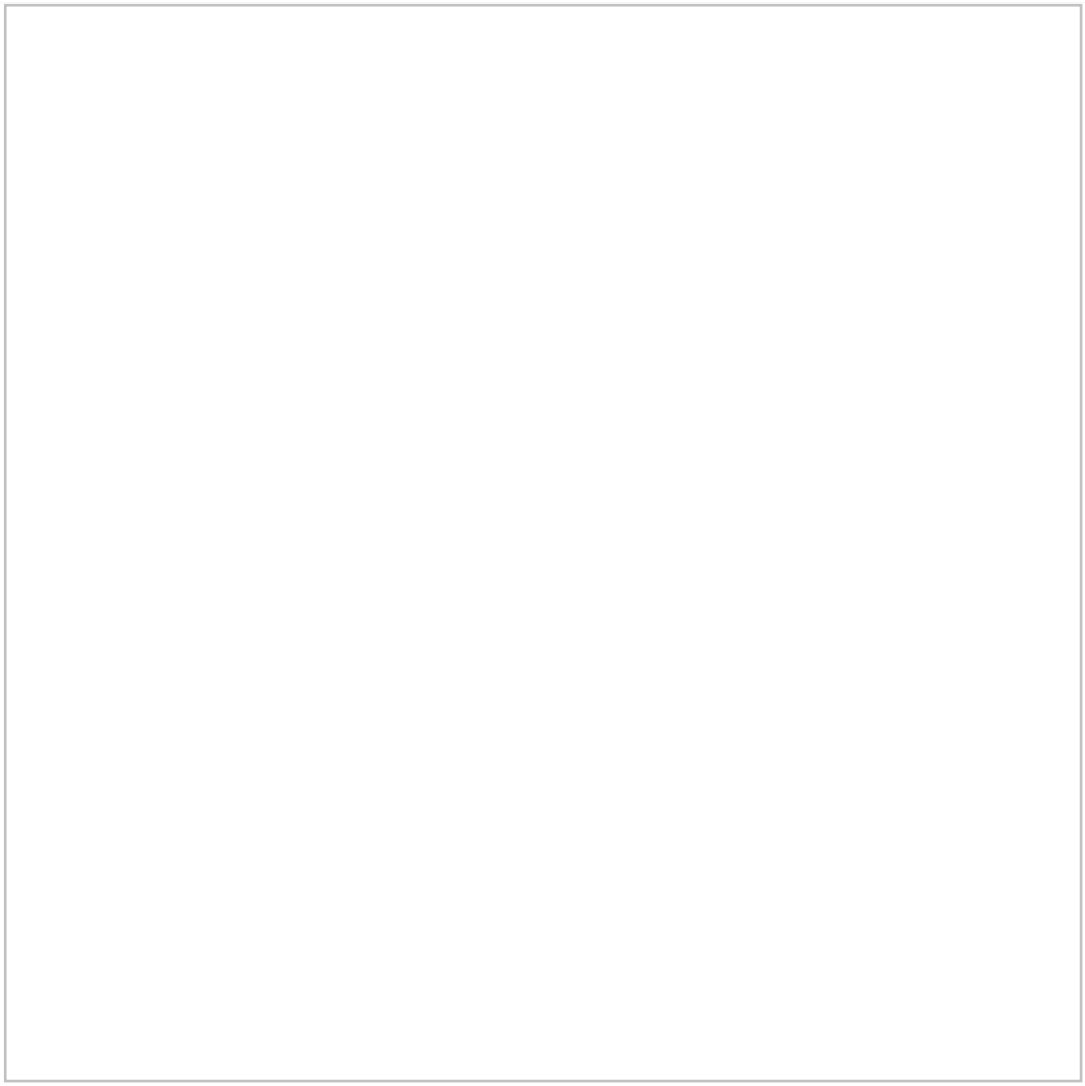
PINGED: WikiLeaks founder Julian Assange was arrested this morning, ending his 7-year stay in London's Ecuadorian embassy.

Ecuadorian officials said they were rescinding Assange's asylum because of his **"discourteous and aggressive behavior" and for violating the terms of his stay**, my colleagues James McAuley, Karla Adam and Ellen Nakashima reported.

Assange, who is wanted in the U.S. for his role in leaking government secrets, took refuge in the embassy when he was facing a Swedish rape charge. U.S. officials want to question Assange about WikiLeaks' role in a Russian hacking and disinformation campaign that upended the 2016

election. “Ahead of the U.S. election in 2016, WikiLeaks released tens of thousands of emails that had been stolen from the Democratic National Committee and from Hillary Clinton’s campaign chairman, John Podesta, in cyber-hacks that U.S. intelligence officials concluded were orchestrated by the Russian government,” my colleagues reported.

Assange’s ouster from the embassy was long expected. Ecuadorian officials said last week they would eject Assange at a time of their choosing. “Ecuador has sovereignly decided to terminate the diplomatic asylum granted to Mr. Assange in 2012,” President Lenín Moreno said in a video statement. “The asylum of Mr. Assange is unsustainable and no longer viable.” Moreno specifically cited WikiLeaks leaking of documents from the Vatican in January. WikiLeaks has said the move is retaliation for its reporting on corruption in Moreno’s administration.



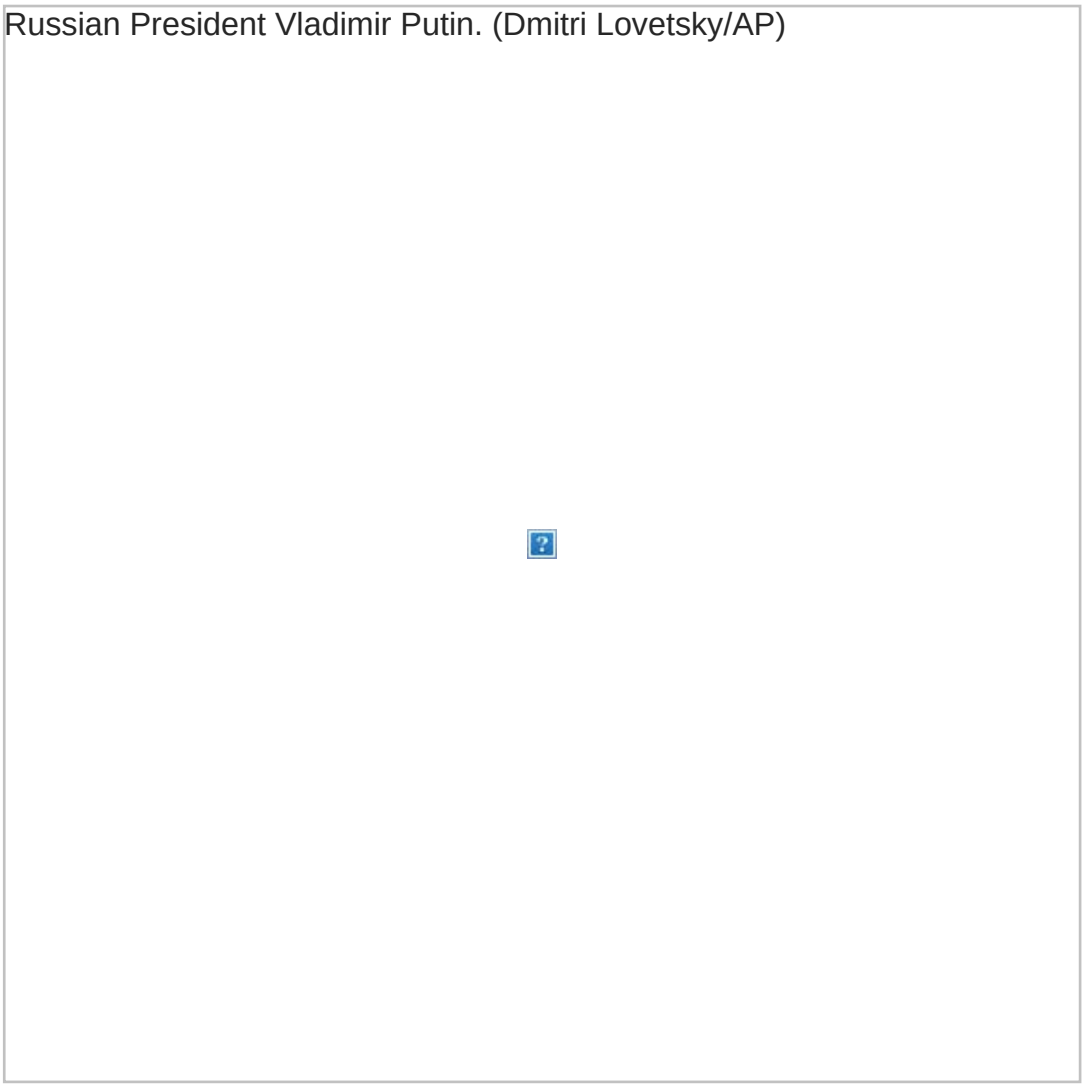
Outgoing Homeland Security Secretary Kirstjen Nielsen, left, and outgoing acting deputy secretary Claire Grady arrive for the dedication ceremony at the Homeland Security headquarters. (AP Photo/Alex Brandon)

PATCHED: A cascade of resignations at the top of the Department of Homeland Security won't damage DHS's cybersecurity mission, Jeanette Manfra, assistant director of the department's Cybersecurity and Infrastructure Security Agency, said Wednesday.

"It's unfortunate to lose Secretary [Kirstjen] Nielsen and [Undersecretary for Management] Claire Grady, who were such great advocates for our mission," Manfra told reporters on the sidelines of a cybersecurity discussion hosted by the Atlantic. "But I think one of the most important things that Secretary Nielsen believed in was resilience and so we're going to continue the mission."

Manfra also praised DHS's new acting chief Kevin McAleenan, who she said worked extensively with technology as commissioner of U.S. Customs and Border Protection and understands the importance of DHS's cybersecurity mission. "I don't see any kind of change to our approach or our ability to do our job," Manfra said.

Russian President Vladimir Putin. (Dmitri Lovetsky/AP)



Russian President Vladimir Putin. (Dmitri Lovetsky/AP)

PWNED: Kremlin-linked hackers likely conducted reconnaissance against election networks in all 50 states before the 2016 contest, according to a Joint Intelligence Bulletin from the FBI and Department of Homeland Security obtained by Ars Technica's Sean Gallagher.

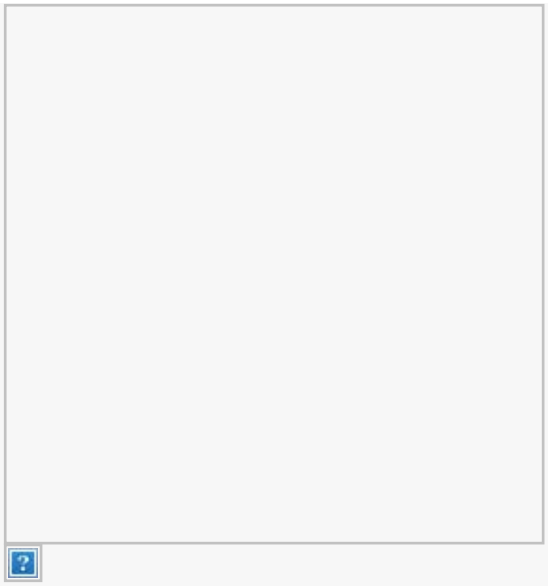
That's the first official report from the agencies that Russian hackers probably probed more state election networks than the 21 identified

in 2016. But it's basically in line with what DHS officials have long said: The Russian reconnaissance mission probably was larger than what the government detected because the federal government's network of sensors on state election systems was not well developed at the time. That network covered more than 90 percent of state election systems by the 2018 midterms, officials have said.

The new bulletin does not alter DHS and FBI's primary conclusion: that there's no evidence Russian hackers changed any votes in the 2016 election.

Here's more from Sean, who credited the paywalled intelligence newsletter Ooda Loop for first reporting on the bulletin, which "stated that, while the FBI and DHS 'previously observed suspicious or malicious cyber activity against government networks in 21 states that we assessed was a Russian campaign seeking vulnerabilities and access to election infrastructure,' new information obtained by the agencies 'indicates that Russian government cyber actors engaged in research on — as well as direct visits to — election websites and networks in the majority of US states.' "

"While not providing specific details, the bulletin continued, 'The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US states' election networks leading up to the 2016 Presidential elections.' "



PUBLIC KEY

How much does it cost to steal a tax refund? Very little, according to research by the cybersecurity firm Carbon Black, which scoured dark Web marketplaces frequented by scammers who steal enough of a person's information to file a phony tax return and collect the refund.

"W-2s and 1040s are available on the dark web at relatively low cost, ranging from $1.04 to $52," Carbon Black reported. "Names, Social Security Numbers (SSNs) and birthdates can be obtained for a price ranging from $0.19 to $62."

The company also found how-to guides for filing false tax returns for about $5.

Carbon Black recommends the standard slate of security measures for consumers to protect themselves against scammers filing phony returns on their behalf, such as being cautious about sharing their information and using multi-factor authentication tools to access email and social media accounts that might contain that information.

Another common piece of advice is for taxpayers to file early before a scammer does it for them. Unfortunately, the report — timed with the April

15 filing deadline — is coming a bit late for that advice.

More cybersecurity news from the public sector:

German stance on 5G security a 'positive step forward': U.S. official

The United States wants foreign governments to follow Germany in adopting strict...

Reuters • **Read more »**

Attorney general says he believes ‘spying did occur’ in probe of Trump campaign associates

Law enforcement officials have defended their handling of the Russia investigation, and they have denied they engaged in political spying.

Devlin Barrett and Karoun Demirjian • **Read more »**

Who is the man behind Huawei and why is the U.S. intelligence community so afraid of his company?

Ren Zhengfei turned a company with no intellectual property into the world’s largest telecom and made China a global leader in 5G technology. Washington says he had help from Beijing.

Los Angeles Times • **Read more »**

U.S. Officials Pressure Russia-Linked Buyout Firm to Sell Stake in Cybersecurity Company

U.S. national security officials told a private-equity firm partly backed by a Russian billionaire named in the Steele dossier

to sell its stake in cybersecurity firm Cofense.
Wall Street Journal • **Read more »**

Pentagon Says No JEDI Conflict, Narrows Field to AWS and Microsoft

The Pentagon's Joint Enterprise Defense Infrastructure cloud contract could be awarded by mid-July.
Nextgov • **Read more »**

National Guard looks to industry for weekend cyber warriors -- FCW

The National Guard wants to increase cybersecurity capacity by attracting exiting servicemembers and full-time private-sector professionals.
FCW • **Read more »**

PRIVATE KEY

Cybersecurity news from the private sector:

Yahoo to pay $117.5M in latest settlement of massive breach

Nearly 200 million people ensnared in Yahoo data breach eligible for up to $117.5 million in free services, other potential restitution
Michael Liedtke | AP • **Read more »**

U.S. government issues warning about new North Korea-linked malware - CyberScoop

DHS and FBI officials are warning industry about what they say is North Korean-liked malware that's been deployed as part of their global operations.

Cyberscoop • **Read more »**

Two out of three hotels accidentally leak guests' personal data:...

Two out of three hotel websites inadvertently leak guests' booking details ...

Reuters • **Read more »**

New APT group TajMahal operates as a 'full-blown spying network,' Kaspersky says - CyberScoop

Researchers have uncovered an advanced persistent threat that for at least five years has used an array of hacking tools and covert automatic updates as part of a hacking campaign that bears little technical similarity to any other APT.

Cyberscoop • **Read more »**

Researchers Find New Victim of 'Triton' Hackers

A security firm has discovered a new victim of the infamous hacking group that targeted critical infrastructure with destructive malware.

Motherboard • **Read more »**

How Android Fought an Epic Botnet—and Won

The Chamois botnet once infected 20 million Android devices. Here's how Google finally broke it up.

Wired • **Read more »**

Share The Cybersecurity 202: Twitter Facebook

Trouble reading? Click here to view in your browser.

You received this email because you signed up for The Cybersecurity 202 or because it is included in your subscription.

Manage my email newsletters and alerts | Unsubscribe from The Cybersecurity 202

Privacy Policy | Help

The Washington Post

Democracy Dies in Darkness

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Maria Benson; Milhofer, John; Lindsey Forson
Subject:	NASS Elections Committee Alert: DHS I&A Input on Foreign Influence Activities, Klobuchar Letter to DHS/FBI re Task Force on Misinformation/Disinformation, 50 States are Targets, Brennan Center Report on AVR
Date:	Friday, April 12, 2019 12:13:21 PM
Attachments:	(FOUO) Survey on Foreign Influence Activities.pdf NASS Communications 2016 Foreign Election Targeting--FW The Cybersecurity 202 Companies are trying to crack down on shady apps that spy on partners exes.msg Message from the EI-ISAC - (UFOUO) Joint Intelligence Bulletin - New Information Reveals Russian Government Cyber Actors Likely Conducted Research and Reconnaissance Seeking Vulnerabilities in All US States" Election Infrastructure in 2016 - UFOUO.msg
Importance:	High

Dear NASS Elections Committee, Communications Directors and IT Directors:

DHS Intel Cyber Mission Center Requests Input on Misinformation/Disinformation Campaigns

(U/FOUO) The DHS Intelligence Cyber Mission Center (CYMC) tracks ongoing overt and covert influence activities, including a limited number of social media accounts suspected of being controlled by foreign influence actors, (foreign) state controlled media and other (foreign) state government affiliated websites.

The CYMC is requesting feedback from partners to better understand the value and use of reporting on suspected state-sponsored influence operations targeting US audience. I&A is seeking to identify whether providing DHS stakeholders with insight into foreign influence activities—including trending topics and hashtags across social media platforms, state media, and suspected influence websites—would be valuable for those entities to carry out their missions and operations. The attached survey questions should only take a few minutes, and are intended to help us assess the value of this reporting, the precise intended audience, and how it may be used by relevant stakeholders to accomplish mission-related tasks.

NASS would encourage you to respond to the survey questions – it's a one-page survey. We have been working with DHS, social media companies, and others to develop useful resources to help identify and share misinformation/disinformation, which we will share at the 2019 Summer Conference. This would be an important piece of the puzzle. Feel free to have multiple responses come from your office.

Sen. Klobuchar Sends Letter to FBI and DHS Urging Joint Task Force on Misinformation/Disinformation

On a related note, Sen. Klobuchar's office shared with us a letter she has sent to DHS and FBI urging them to form a joint task force to include social media platforms and state and local election officials to help identify and address misinformation/disinformation. NASS suggested something similar in our letters to Facebook and Twitter after their appearance at the NASS 2019 Winter Conference.

News Stories on all 50 States as Targets

We shared this information with your communications directors yesterday, but we wanted to share with you as well. Attached you will find the email to the comms directors.

Yesterday, the *Washington Post* cybersecurity newsletter said the intelligence community has made

the assessment that malicious Russian-linked actors likely targeted all 50 states' election networks in 2016, instead of the original 21 identified. **This is not new information**, as the Department of Homeland Security (DHS) has been saying this was likely for quite some time. Former DHS Secretary Nielsen also said this at the 2018 NASS Summer Conference during her keynote speech. In addition, NASS has been consistently saying all 50 states consider themselves a target and states have acted accordingly to further secure and protect their election networks and systems. This latest intelligence assessment does not change the original conclusions that 1) only one state's voter registration database was partially breached, which changed no voter information and did not result in problems voting; and 2) no votes were changed in the 2016 election.

We have also attached the EI-ISAC alert with the Joint Intelligence Bulletin that went out to everyone March 29th.

Brennan Center Releases Newest Report on AVR

Today we received this report from the Brennan Center: AVR Impact on State Voter Registration. If you have any questions about the report, please contact Natalie Tennant, tennantn@brennan.law.nyu.edu

Thanks,
Leslie

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee Alert: DHS National Virtual Tabletop Important Notice, DHS" CISA Releases Best Practices, Risk Limiting Audit Guides, House Hearings, NVRD Mentor Program
Date:	Friday, May 24, 2019 4:45:42 PM
Attachments:	Mentor Partner RFP - NVRD 2019.docx
Importance:	High

Dear NASS Elections Committee Members, Communications Directors and IT Directors:

I hope you are off on a fabulous long-weekend adventure instead of reading this email☺

DHS National Virtual Tabletop (TTX)– June 18, 19, 20 – Important Reminders

1. **You must test your video link for the tabletop by next Friday, May 31st.** Once done, you must email CEP@hq.dhs.gov. This is VERY important
2. Please remember, this **TTX is CLOSED TO PRESS**.
3. TTX materials and final information will be sent out on June 12, 2019.
4. If you would like any of your election vendors to participate with you, you must invite them.

DHS' Cybersecurity and Infrastructure Security Agency (CISA) Shares Best Practices for Securing Elections Systems and Self-Assessment Questionnaire

Here is a link to Best Practices developed by CISA. These practices were developed by their Hunt Incident Response (HIRT) Teams.

These practices are based on risks and vulnerabilities the HIRT teams saw when doing work with state and locals on their election infrastructure and with other state and local agencies. These practices are actionable, low or no-cost, and will help address vulnerabilities and prioritize resources.

Risk-Limiting Audit Report "Knowing It's Right" Released – Parts 1 & 2 – More to Come

We have heard from Jennifer Morrell on her work on Risk Limiting Audits with the states at a couple of our conference. Here are links to her much anticipated reports:

Knowing It's Right Part I: A Practical Guide to Risk Limiting Audits provides a higher level overview for state and local stakeholders who want to know more about RLAs before moving on to the implementation phase

Knowing It's Right, Part Two: Risk-Limiting Audit Implementation Workbook serves as a complementary workbook on how to conduct the ballot-comparison audit.

House Admin hearing on EAC Oversight

On Tuesday, May 21st, the House Administration Committee held an EAC Oversight hearing. You'll remember that Senate Rules had a similar hearing last week. EAC funding and staffing, the VVSG 2.0, Terms of Executive Director and General Counsel and employee issues were all discussed at length.

House Oversight Committee's National Security Subcommittee holds a hearing on Election Security and Preparedness

On Wednesday, May 22nd, the House Oversight's Subcommittee on National Security held a hearing "Securing U.S. Election Infrastructure and Protecting Political Discourse. Witnesses included:

The Honorable Christopher Krebs, Adam Hickey, The Honorable Christy McCormick, The Honorable Ellen L. Weintraub, The Honorable Bill Galvin, Richard Salgado, Nathaniel Gleicher, Kevin Kane
Most of the focus of the hearing was on the actions of the witnesses from Twitter, Google and Facebook.

National Voter Registration Day (NVRD) implements Mentorship Program to Assist Organizations New to Voter Registration
I have been asked by NVRD to share this information on a pilot mentorship program they are launching.

"Attached is an RFP for a pilot project National Voter Registration Day is running in 2019. It's a Mentorship program aimed at supporting community partners who are new to doing voter registration work. Our surveys from last year showed that 34% of the partners who signed on said they had not done voter registration work before. The Mentorship program seeks to identify local Mentor Partners – nonpartisan organizations and election offices with expertise in the space – to provide additional support to those groups that are new to doing this work, from helping them set realistic goals to ensuring registration forms are collected and turned in properly."

Have a wonderful Memorial Day weekend.

Best,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Maria Benson; Milhofer, John; Lindsey Forson
Subject:	NASS Elections Committee: Bipartisan Senate Bill "Protect our Elections Act", DARPA and Galois to Design Open Source Voting System, Customizable Risk Limiting Audit Tool by VotingWorks
Date:	Monday, March 18, 2019 3:42:53 PM
Attachments:	summary-protect-elections-act-031819.docx
Importance:	High

Dear NASS Elections Committee and IT Directors:

Senate Bipartisan "Protect Our Elections Act" introduced in the Senate

Last Thursday, Senators Van Hollen (D-MD), Collins (R-ME), Cardin (D-MD) and Rubio (R-FL), introduced Protect our Elections Act. The bill is not yet posted with a number. See attached NASS summary.

Much of this bill mirrors legislation introduced last Congress by these members. The bill calls for DHS and EAC to develop cybersecurity best practices for election service providers, qualified election service providers must meet a series of requirements including US ownership, EAC must maintain a list of qualified election service providers, each state/local jurisdiction must check EAC list to ensure they are using qualified election service providers.

DARPA and Galois to partner on Open Source Voting System Design

Last week, several news outlets reported that the US Defense Advanced Research Projects Agency (DARPA) has partnered with Oregon-based contractor Galois to design an open-source security voting system. DARPA has committed $10 million to the development of this system. We will be tracking down more information on this project and share it when we have it.

VotingWorks to Develop Risk Limiting Audit (RLA) Tool For Use by All States

Many of you may have read in electionline last week about a new open-source resource coming for RLAs. VotingWorks will help interested states to utilize an RLA tool that can be customized for different election environments (central/precinct count, voting systems, etc.) As with the DARPA project, we are working to track down more information on this project and share it when we have it.

Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

Disclaimer

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Maria Benson; Lindsey Forson; Milhofer, John
Subject:	NASS Elections Committee: Chair Lofgren Requests State Reports on HAVA Spending since 9/2018, GCC Update and Resources, EAC Alert on Closing Out HAVA Funds pre 2018 Disbursement
Date:	Wednesday, April 10, 2019 5:47:18 PM
Attachments:	4.10.19 Letter to State Elections Officials - Final.pdf DMARC FINAL 20190325.pdf Multi-Factor Auth FINAL 20190325.pdf .gov one pager FINAL 20190402.pdf
Importance:	High

Dear NASS Elections Committee, Communications Directors and IT Directors:

Letter From Chair Lofgren Requesting Info on State Spending of HAVA $ since September 2018

House Administration Chair Zoe Lofgren (D-CA) sent us the attached letter today and asked that we share with you. She is asking for details on HAVA funding spent since September 2018. Sec. Condos will be preparing a response from NASS to send to Chair Lofgren, but the letter asks each of you to respond regarding the circumstances in your state. She asks that responses to her are completed by May 15, 2019. Any responses can be sent to Tanya Seghal, Majority Elections Counsel, tanya.sehgal@mail.house.gov

New Regular Updates from the EIS-GCC

The EIS-GCC Executive Committee has asked that a regular update go out to all EIS-GCC members. This new update will go out bi-weekly.

- **Updates from GCC-SCC Joint ExCom Meeting**

  The GCC and SCC Executive Committees met on Wednesday, April 3 to discuss shared goals and a collaborative path forward between now and Election Day 2020. The two groups identified a preliminary set of goals and committed to establish a joint working group to update the GCC's 2018 Sector-Specific Plan (SSP) to reflect those goals in a joint document. The Working Group's goal is to bring the completed document to both councils for a final vote before the end of 2019. Once the joint SSP is finalized, the councils will develop implementation strategies, either jointly or individually as appropriate. Next update, we will provide more specific progress updates from the GCC and Joint Working Groups, which are open to your participation as your schedules allow.

- **Election Security Clearance Program Update**

The Cyber and Infrastructure Security Agency (CISA) is initiating the "Plus 3" phase of its election security clearance program, which will provide additional clearance opportunities for state and local government officials and private sector election infrastructure partners.

Three additional election officials in each state will be nominated via the following process:

- A state or local election official, nominated by the state chief election official;
- The local representative to the EAC Standards Board (or their designee) in the state; and
- A state or local election official, nominated by CISA regional staff (e.g. a Regional Director or Protective Security Advisor).

CISA will coordinate with the EIS GCC to ensure awareness and that the appropriate individuals are nominated. Nomination opportunities will also be available for up to three Private Sector election infrastructure partners in each state, as nominated by CISA regional staff. CISA will coordinate with the EISCC to ensure their awareness and ensure the appropriate individuals are

nominated.

- **New Election Security Products Published**

CISA's Election Security Initiative has recently published a series of slick sheets (attached to this email) on cybersecurity practices state and local election officials can implement to enhance their organizational cybersecurity posture. Covered topics include:

- Doman-based Message Authentication, Reporting, and Conformance (DMARC);
- Multi-Factor Authentication; and
- Leveraging the .gov Top-Level Domain.

From the EAC – Closing Out HAVA funds (distributed before 2018)

We are sharing this alert we received from the EAC's Mark Abbott (mabbott@eac.gov)

The grants office at the Election Assistance Commission has been working over the last year to close out all old HAVA awards. This project is nearing its conclusion and we will be sending you detailed, state-specific instructions for closing awards in the coming weeks. Once you receive your letters via email, Peg, Mike and I will be available to answer any questions you may have. This email is to make sure everyone has a practical understanding of what this process means for their state/territory, so please note the following:

1. This process will not result in your states/territories losing funds. If you have unspent Section 101 or 251 funds, the balances, along with any accrued interest and state match obligations will be transferred to a new award.
2. 2. If you have unclaimed Section 251 Funds sitting with the EAC, those funds will be sent to you after the new grant awards are issued, unless you opt not to receive those funds at this time. With a few notable exceptions, the amounts available from the EAC are less than $20,000.
3. For all grants being closed, the three-year federal record retention clock will begin the day you receive our notice. This will close grants that have, in many cases, been open over 15 years. There may also be implications for special equipment dispensation. EAC guidance regarding equipment can be found here.
4. We have designed this process to reduce or eliminate any additional burden on states/territories but there will still be several items on your to-do list if we issue a new award with your remaining balances.
5. This process has nothing to do with the 2018 awards you just received.

Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Maria Benson; Milhofer, John; Lindsey Forson
Subject:	NASS Elections Committee: Federal Legislation, Procurement Guides, Talking Points Post-Mueller Report
Date:	Friday, March 29, 2019 4:39:53 PM
Attachments:	Cybersecurity General Talking Points-March 2019.pdf
Importance:	High

Dear NASS Elections Committee, IT Directors and Communications Directors:

For the People Act Moves to the Senate

HR 1, For the People Act which passed the House earlier this month has been introduced in the Senate by Sen. Udall (D-NM). Media reports say the bill has support from all 47 Democratic Senators. However, Senate Majority Leader McConnell has made public statements that the bill will not move forward in the Senate. Still nothing in the Senate regarding the reintroduction of the Secure Elections Act.

Procurement Guides Issued by The Brennan Center and the Center for Internet Security (parent co of the EI-ISAC)

To assist state and local officials with procurement processes that include enhanced/baked-in cybersecurity provisions, a few resources have been or are in the process of being developed. The Brennan Center has just released their Procurement Guide for election officials.

Additionally, The Center for Internet Security (CIS) will soon release their Procurement Guide. The two guides will complement one another, but the CIS guide will be more detailed and comprehensive. The CIS guide will be shared at the NASS Tech Talk on April 15th by Mike Garcia. It will be officially released at the end of April at the MS-ISAC/EI-ISAC conference in Denver.

TurboVote Letter to Chief State Election Officials re 2018

TurboVote sent a letter to chief state election officials this week responding to questions about 2018 issues posed to them at the NASS 2019 Winter Conference. They planned to send the letter to the communications director in your office because of the availability of their email address. NASS does not share Secretaries email addresses.

EI-ISAC Members and Partners Report Receiving Phishing Emails

From EI-ISAC (If you need me to share EI-ISAC full email, let me know)

"Multiple EI-ISAC members and partners reported receiving phishing emails from cloud storage accounts associated with a local election official. One of the emails included a Dropbox link and the second linked to a Microsoft OneDrive file. When a user visits either of these links, they open a file directing them to the same Office 365 credential harvesting page. As this is a common technique, there is not enough information at this time to determine this activity strategically targeted election officials.

Credential harvesting phishing emails are a common malicious email campaign affecting organizations in all sectors. Credential harvesting emails attempt to trick users into entering their credentials into a fraudulent website to steal their login information. After entering the credentials, the user is often redirected to a legitimate webpage. These emails are more likely to reach email

inboxes and trick users if they originate from legitimate accounts, such as potentially compromised accounts. In the reported emails, the subject and body used the common lure of sharing an invoice or statement with the recipient. Both emails also appeared to originate from legitimate accounts, indicating a potential compromise of the originating government accounts."

NASS Election Security Talking Points re Federal State and Local Efforts

After the release of Attorney General Barr's letter summarizing the Mueller Report, we updated our talking points. We shared the talking points with communications directors earlier this week, but wanted to share them again with you. We believe it is important to reiterate that all 50 states consider themselves a target for bad actors in 2020 and are preparing accordingly.

Have a good weekend and enjoy some college basketball!

Best,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee: House Admin Hearing Tomorrow on Election Security, Ryan Macias, Acting Director of Testing and Certification Leaving EAC, Chair Lofgren Letter - State Responses
Date:	Tuesday, May 07, 2019 11:22:22 AM
Attachments:	4.10.19 Letter to State Elections Officials - Final.pdf
Importance:	High

Dear NASS Elections Committee:

House Admin Hearing on Election Security at 2PM ET on Wednesday, May 8, 2019

This morning we learned of a House Administration Committee hearing on Election Security at 2PM tomorrow, May 8, 2019.

The witness list was just released. It includes:

Larry Norden, Brennan Center for Justice
Marian Schneider, Verified Voting
Joseph Lorenzo Hall, Center for Democracy and Technology
Secretary Jocelyn Benson, Michigan Secretary of State
Secretary John Merrill, Alabama Secretary of State

This hearing is happening at the same time as a markup on the Corporate Transparency Act in House Financial Services which impacts Secretary's Business Services offices. We will cover both hearings and send you any relevant outcomes.

EAC Acting Director of Testing and Certification to leave EAC

We also learned this morning that Ryan Macias, Acting Director of Testing and Certification, will leave the EAC on May 17, 2019. Ryan has served as Acting Director since the departure of Brian Hancock, former Director of Testing and Certification. After May 17, 2019, any questions regarding testing and certification should be directed to Jerome Lovato (jlovato@eac.gov).

State Responses to Chair Lofgren's HAVA Spending Letter

If your office has responded to Chair Lofgren's letter (attached) and you are willing to share with other states, please send along to me. I have received requests by states for examples of other state's letters. Here is the NASS response to Chair Lofgren.

Busy morning…..
Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525

www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee: House Approps on Election Security, President"s FY2020 Budget Request, Dark Web, DNC/RNC Conventions Set for 2020, USPS Mail Ballot Event Agenda/Registraiobn
Date:	Wednesday, March 13, 2019 1:46:31 PM
Attachments:	2019 NPF Featuring a Special Election Mail Forum.docx
Importance:	High

Dear NASS Elections Committee Members:

House Appropriations Subcommittee on Homeland Security hearing "Securing Federal Networks and State Election Systems" today at 2PM EDT

CISA Director Chris Krebs will testify today at 2PM EDT at House Appropriations Subcommittee on Securing Federal Networks and State Election Systems
Live-stream can be found here: https://youtu.be/WvyK0fNqVUM

President's FY 2020 Budget Request

The President's FY 2020 Budget Request does not include specific reference to any funding for election security, meaning no reference to state payments. However, it does reference funding for DHS, which has been used to support the elections community.

"Supports the Cybersecurity of Government Networks and Critical Infrastructure. The President's National Cyber Strategy highlighted DHS's role in securing and building cybersecurity resilience for the Nation's most critical infrastructure, including government networks. DHS works with key partners and stakeholders to identify and manage national cybersecurity risks. The Budget includes more than $1 billion for DHS's cybersecurity efforts. These resources would increase the number of DHS-led network risk assessments from 473 to 684—including assessments of State and local electoral systems—as well as for additional tools and services, such as the EINSTEIN and the Continuous Diagnostics and Mitigation programs, to reduce the cybersecurity risk to Federal information technology networks."

Mr. Krebs will be discussing this at the House Approps hearing today.

Update on Dark Web Claims

DHS and the EI-ISAC continue to see claims that voter registration data is available on the Dark Web. We began to see these claims made in the Fall of 2018. As we have been told, claims happen much more frequently than actual incidents. However, it is advisable to be vigilant. Please reach out to DHS (ncciccustomer@hq.dhs.gov) and/or EI-ISAC (soc@cisecurity.org) for any assistance they may be able to provide.

DNC and RNC 2020 National Convention Dates and Locations Set

It was announced yesterday that the DNC has selected Milwaukee, WI for their 2020 National Convention, which will take place from July 13-16, 2020. The Republicans will hold their 2020 National Convention in Charlotte, NC from August 24-27, 2020. We would note that NASS reauthorized our resolution **Urging the National Political Parties to Set Earlier Nominating Convention Dates,** which we sent to the parties in the summer of 2018.

National Postal Forum/USPS Event on Mail Ballots – May 6, 2019 in Indianapolis, IN

Attached you will find an agenda and registration information for the NPF/USPS on May 6, 2019. There is a special rate for election officials of $99.

Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee: NGA Launches Policy Academy on Election Cybersecurity, Belfer"s D3P After Action Review of 2018, NonProfit Vote and US Elections Project Report on 2018 Turnout, EAC Annual Report
Date:	Friday, March 22, 2019 5:04:03 PM
Attachments:	Request for Applications - NGA Policy Academy on Election Cybersecurity.pdf D3P DecCon AAR Report v2.0 INTERNAL.PDF
Importance:	High

Dear NASS Elections Committee, IT Directors and Communications Directors:
Attached/linked are some reports and opportunities for your review.

National Governors Association Center for Best Practices Launches Policy Academy on Election Cybersecurity – Application Attached

The National Governors Association Center for Best Practices (NGA Center) is pleased to announce the launch of its ***Policy Academy on Election Cybersecurity***. Please see the attached document for full details. **Applications must be submitted in PDF format to Maggie Brunner (mbrunner@nga.org) no later than 8:00 PM ET, May 10, 2019.** Please direct any questions to Maggie Brunner (mbrunner@nga.org; 202-624-5364), David Forscey (dforscey@nga.org; 202-624-5356), or Michael Garcia (mgarcia@nga.org; 202-624-5312).

This project will competitively select **five states** to participate in a policy development process to maximize public confidence in elections by reducing technical risks to election systems and improving coordination between election officials and state cybersecurity leaders in the executive branch. An NGA policy academy is a highly collaborative, team-based process for helping a select number of states develop and implement action plans that address complex public policy challenges. Participating states receive guidance and technical assistance (e.g., facilitated workshops, policy research, written products) from NGA Center staff and, as appropriate, access to subject matter experts from the private sector, research organizations, academia, and the federal government. A policy academy provides a forcing mechanism that focuses the time and attention of stakeholder groups that can prove difficult to convene under normal circumstances. The strategies and policies developed by participating states are intended to catalyze wider adoption of promising practices across the United States.

The *Policy Academy on Election Cybersecurity* will benefit from direct research support provided by staff and faculty from the University of Southern California. *This project is not an academic study, and no state-specific findings or conclusions will be published or otherwise shared or discussed publicly without the express consent of participating states and other relevant stakeholders.*"

The NGA Center will hold two informational calls to address any questions or concerns about the *Policy Academy*:
1st Informational Call: 3:00 PM ET, April 5, 2019
2nd Informational Call: 2:00 PM ET, April 18, 2019
Conference Number: 888-858-6021
Conference Code: 202-624-5356

Belfer Center's Digital Democracy Center Releases After Action Review (AAR) of 2018 – Please

only share within your office and with local election offices

Attached you will find the AAR of the 2018 Election based on a meeting held at Belfer in December 2018, in which a number of state and local election officials participated. The report shares discussions and proposed practices for implementation moving into the next election cycle. This is a document that is meant for your office and your local election officials. Please do not share beyond these audiences.

NonProfit Vote and US Elections Project Release Report on 2018 Midterms

NonProfit Vote and the US Elections Project have released a joint report, *America Goes to the Polls* which outlines turnout for the 50 states and looks at the impact of Same Day Registration, AVR and Vote by Mail on turnout.

EAC Annual Report Highlights State Activities

The EAC has asked that we share their 2018 Annual Report which features a number of activities with states.

Happy 1st March Madness Weekend!
Best,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee: Several Election-Related Hill Hearings, New Federal Election Legislation, EAC Public Hearing on VVSG, EAC Public Meeting on 5/20, New EAC Testing and Certification Director
Date:	Tuesday, May 14, 2019 5:48:58 PM
Attachments:	summary-election-security-act-2019.docx Voting-System-Cybersecurity-Act-2019-Peters.pdf SERVIS Final.pdf
Importance:	High

Dear NASS Elections Committee:

As usual, a lot to share with this committee.

Senate Rules Committee Hearing tomorrow, Wed. May 15, 2019 at 2:30 PM on EAC Oversight

Tomorrow, the Senate Rules Committee will hold a hearing on Oversight of the EAC at 2:30 PM.
Witnesses:
Chairwoman Christy McCormick, Vice Chair Ben Hovland, Commissioner Tom Hicks, Commissioner Don Palmer

EAC will hold Final Public Hearing on the VVSG 2.0 on Mon. May 20, 2019 from 1:30PM – 4PM ET

The EAC will hold their final Public Hearing on the Voluntary Voting System Guidelines 2.0. This hearing will be live-streamed.
Witnesses:
Honorable Paul Pate, Secretary of State, Iowa
Traci Mapps, Director of Operations, SLI Compliance
Jack Cobb, Laboratory Director, Pro V&V
Joseph Lorenzo Hall, Chief Technologist and Director of the Internet Architecture Project, the Center for Democracy and Technology

House Government Oversight National Security Subcommittee Election Security Hearing on Wed. May 22, 2019 at 2PM

We learned last evening that the National Security Subcommittee of the House Government Oversight Committee plans to hold a hearing on election security. The hearing is not posted yet, but we understand there will be two panels. The first panel will consist of federal officials from DHS, EAC, DOJ and the FEC, and possible others. The second panel will include state election officials, Twitter, Facebook and Google. Apparently the invites are out for the state election officials. As we learn more, we'll keep you posted.

Reps. Thompson (D-MS) and Lofgren (D-CA) introduce the Election Security Act of 2019

Yesterday, we read that Reps. Thompson and Lofgren introduced the Election Security Act of 2019. The bill is not posted online yet, so we don't have a bill number. Attached is a NASS summary of the bill. This is the election security language pulled from HR 1.

Sen. Peters (D-MI) Introduces the Voting System Cybersecurity Act of 2019

We told you on April 30th that Sen. Peters (D-MI), Ranking Member of the Senate Homeland Security and Governmental Affairs Committee (HSGAC), planned to introduce legislation that would add a

DHS representative with cybersecurity expertise to the EAC's Technical Guidelines Development Committee (TGDC). Today, he introduced that legislation (attached). Again, the bill is not posted online, so there is no bill number. The TGDC helps to draft the Voluntary Voting System Guidelines (VVSG). The TGDC currently consists of a Chair (NIST), and representatives from the EAC Standards Board and Board of Advisors, the Access Board, NASED, the scientific community, ANSI, IEEE and NASED.

Sen. Klobuchar (D-MN) and Sen. Collins (R-ME) to Introduce the Secure Elections Require Investment in Vigilant Staff Act or SERVIS Act

While we haven't seen an announcement that this legislation has been introduced, we were told it would be happening this week. The Servis Act would requires the EAC to provide grants to eligible institutions such sums as may be necessary to pay eligible certificate program enrollees for each academic year enrolled in an accredited certificate program in election administration or cybersecurity. Authorizes $1 million in FY 2021 and such sums as may be necessary for FY 2022 through 2028. The grant for each certificate program enrollee must be at least 75% of the tuition for the certificate program. At least 85% of the money must be provided to eligible institutions prior to each payment period and must be based on the amount requested by the institutions as needed to pay eligible certificate program enrollees until the EAC determines an alternative payment system that provides payments to institutions in an accurate and timely manner. The provision does not limit the authority of the EAC to use a reimbursement system of payment. Defines "eligible institutions" as institutions of higher learning that offer an accredited certificate program in election administration or cybersecurity. Defines "accredited certificate program in election administration or cybersecurity" as a program in election administration or cybersecurity that leads to a certificate or other nondegree recognized credential at an eligible institution. Defines "eligible certificate program enrollee" as an individual who:

- Is a state or local election official, employee of a state or local election official, or employee of the EAC;
- Certifies to the EAC their enrollment in an accredited certificate program in election administration or cybersecurity;
- submits a receipt or other verification to the EAC of the tuition amount for the certificate program and an application

EAC Names Jerome Lovato as new Testing and Certification Director

Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

Disclaimer

From:	Reynolds, Leslie
To:	Reynolds, Leslie
Cc:	Dodd, Stacy; Milhofer, John; Maria Benson; Lindsey Forson
Subject:	NASS Elections Committee: Summary of House-passed HR 1, GCC Election Security Priorities Leading into 2020
Date:	Thursday, March 14, 2019 2:59:26 PM
Attachments:	summary-hr1-031319.docx Election Security Initiative_ Ready for 2020.pdf
Importance:	High

Dear NASS Elections Committee:

Summary of HR 1 – as Passed by US House of Representatives

As you all know, HR 1, For the People Act, passed the House last week. The bill was on the House floor for a couple of days with a number of amendments debated and voted on. Attached you will find the NASS summary of the final bill with approved amendments added – thank you John Milhofer!

EIS-GCC Election Security Priorities Leading into 2020 – "Ready for 2020"

At their February 1, 2019 meeting, the Elections Infrastructure-Government Coordinating Council (EIS-GCC) revised and approved their priorities for 2020. The document is attached. Just a reminder that NASS has 12 Secretaries on the GCC (8 members, 4 alternates).

Thanks,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
www.nass.org

NASS Summary: Protect our Elections Act 2019 (Bill number not yet assigned)
Re-Introduced on 03/14/19 by Rep. Van Hollen, (D-MD), Rep. Cardin (D-MD), Rep. Collins (R-ME), Rep. Rubio (R-FL)

Effective Date: Elections for Federal Office beginning 2020

Cybersecurity Best Practices

- No later than 90 days after enactment, the EAC and DHS must establish cybersecurity best practices for election service providers and must update the best practices as they consider appropriate.

Ensuring Domestic Ownership and Control of Election Systems

- Each state and local election jurisdiction must ensure that any election service provider that provides, supports, or maintains any component of an election system used in the administration of the election is a qualified election service provider. Each jurisdiction must evaluate election service provider at least once each year to ensure the election service provider is qualified.
- The EAC must establish and maintain a database in which each state and local election jurisdiction can verify whether an election service provider is qualified.
- The EAC and DHS may provide guidance and technical assistance as appropriate to assist each state and local election jurisdiction with Act's requirements.
- Defines an "election system" as a voting system, an election management system, a voter registration website or database, an electronic pollbook, a system for tabulating or reporting election results, an election agency communications system, or any other information system (as defined in section 3502 of title 44, United States Code) that DHS, in consultation with the EAC, identifies as central to the management, support, or administration of a Federal election.
- Defines an "election service provider" as any person providing, supporting, or maintaining an election system on behalf of an election agency, such as a contractor or vendor
- Defines a "qualified election service provider" as an election service provider who meets each of the following criteria, as established and published by the EAC in coordination with DHS:
    - the election service provider is solely owned and controlled by U.S. persons
        - a person is a corporation or business entity that is created or organized under the laws of a country that is party to the UK–USA Agreement for joint cooperation in signals intelligence, military intelligence, and human intelligence, also known as the 'Five Eyes alliance'
        - DHS may waive the requirement with respect to a person who is a U.S. subsidiary of a parent company which has implemented a foreign ownership or control mitigation plan that has been approved by DHS. The plan must ensure that the parent company cannot control, influence, or direct the subsidiary in any manner that would compromise or influence, or give the appearance of compromising or influencing, the independence and integrity of an election.

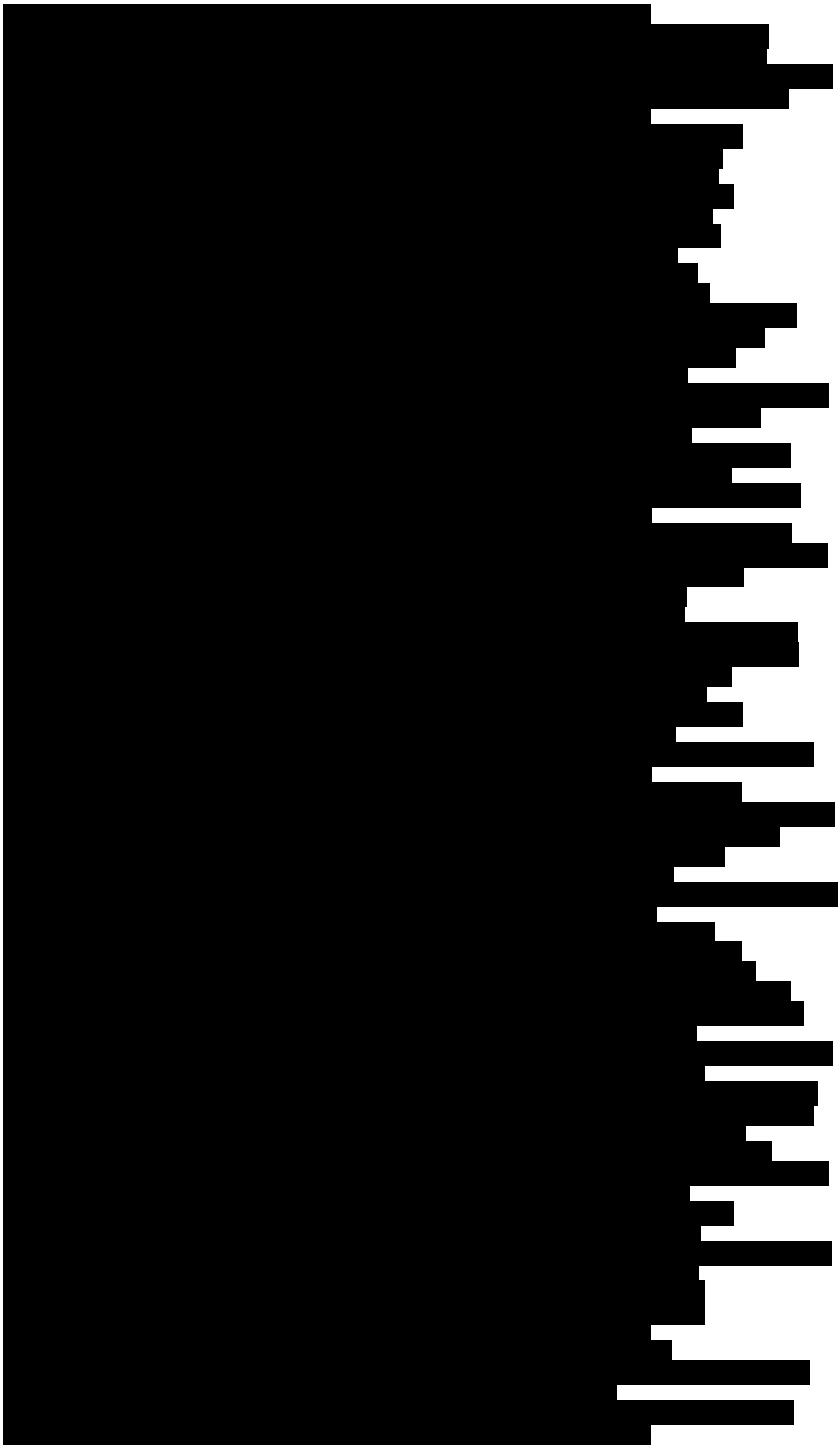
        - the EAC, in consultation with the Secretary of the Treasury, shall issue regulations defining the terms "ownership" and "control"
    - the election service provider submits, in accordance with the ownership information sharing requirements in the Act:
        - notice of any material change in ownership or control of the election service provider and;
        - any other information required to be reported.
    - the election service provider agrees to ensure that the election systems will be developed and maintained in a manner that is consistent with the cybersecurity best practices established by the EAC and DHS
    - The election service provider agrees to maintain its information technology infrastructure in a manner that is consistent with the cybersecurity best practices established by the EAC and DHS
    - the election service provider shall report any known or suspected security incidents involving election systems to the chief state election official of the state involved or the official's designee, the EAC, and DHS

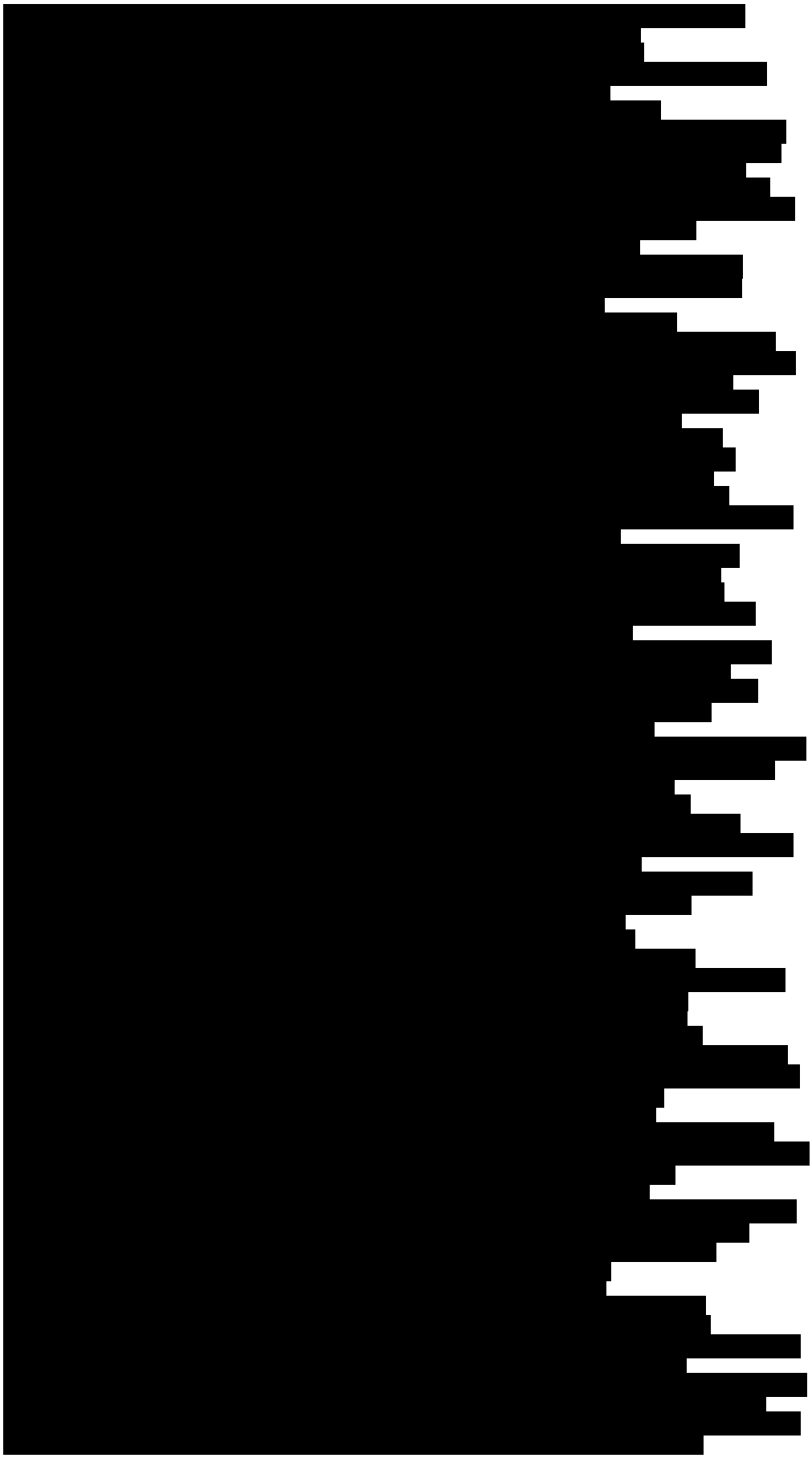
Information Sharing with Respect to Ownership of Election Service Providers

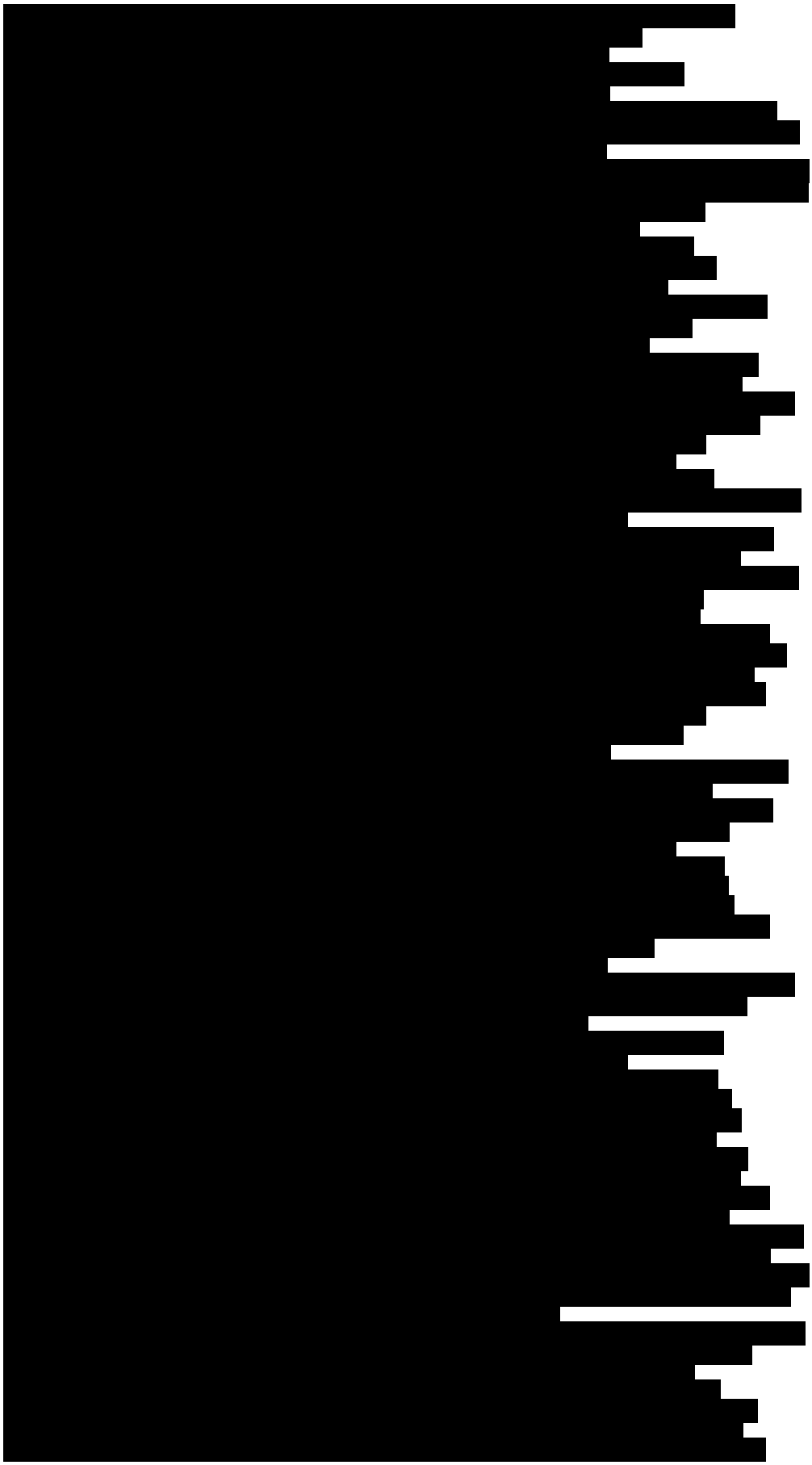
- Defines "appropriate state or local governmental entity'', with respect to an election service provider, as any state or local governmental entity that the election service provider seeks to contract with, contracts with, or otherwise provides services to provide, support, or maintain an election system
- Each election service provider must submit to DHS, the EAC, and the appropriate state or local government entities the following information:
    - no later than 90 days after the date of enactment or the date that a person first becomes an election service provider (whichever is later), a report listing the identity of any foreign national (as defined in section 319(b) of the Federal Election Campaign Act) who directly or indirectly owns or controls such election service provider and the percentage of such ownership, and any other information necessary to determine whether the election service provider is a qualified election service provider
    - no later than 90 days after the date of any material change in ownership or control of such elecion service provider, a notice of such change and an update of any information previously reported.
- If an election service provider fails to submit a report, the Attorney General may, after notice and opportunity for hearing, impose a civil fine of $20,000.

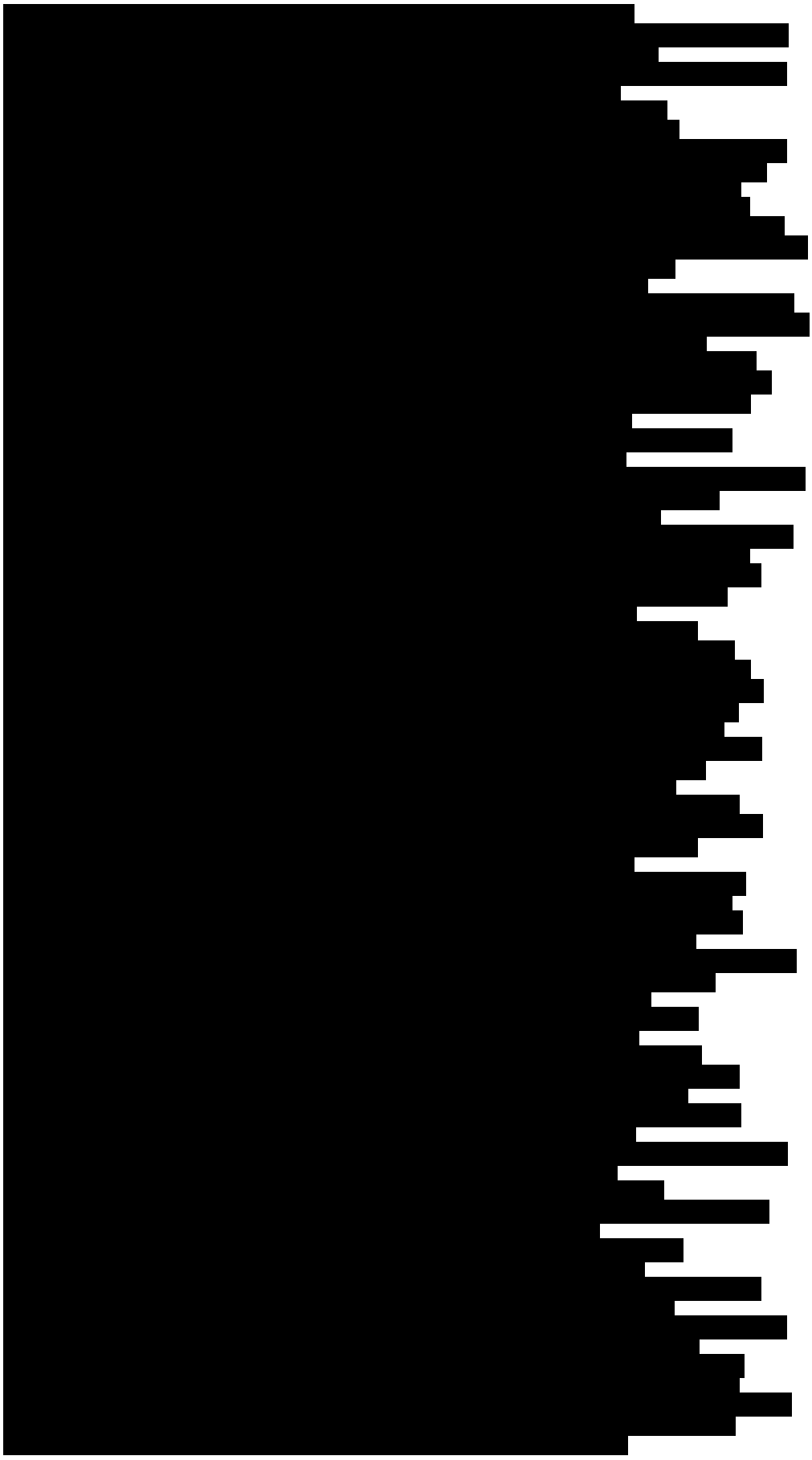
03/18/19

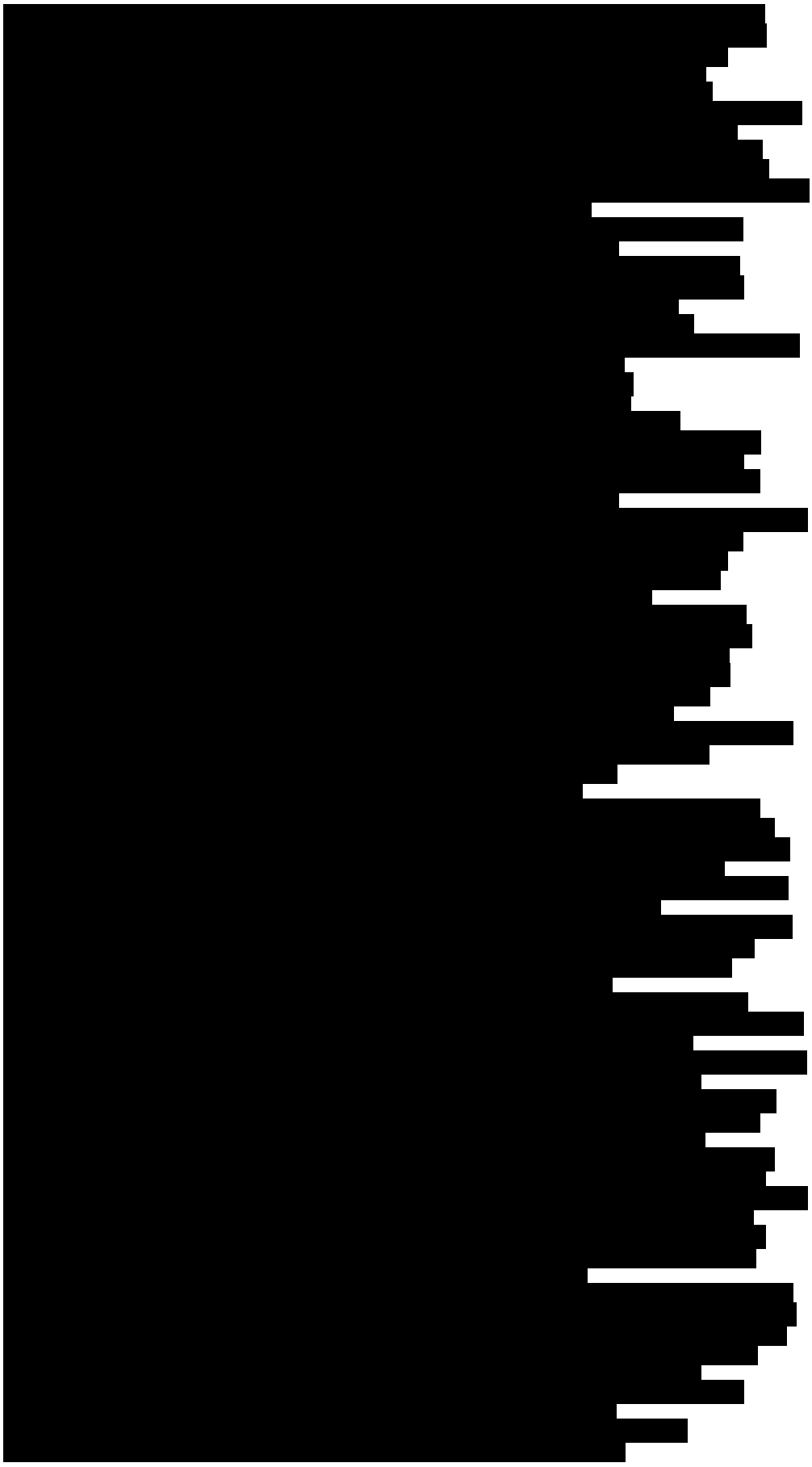
From: Colleen McCormack on behalf of NHVotes
To: NHVotes
Bcc:











[redacted]

Subject: New Request for Access (RAE) Forms and Uncheck 2018 UOCAVA Voters
Date: Thursday, March 07, 2019 10:21:59 AM

Dear Clerks and Supervisors:

1. Every user in Electio*Net* must fill out a new "Request for Access" (RAE) form – See attachment
    - Deadline to return the form is the end of March
        - Please give the completed form to your Town/City Clerk
        - Clerks return the completed form by scanning or faxing to: nhvotes@sos.nh.gov or 271-8242
    - We will be transitioning to "Two Factor Authentication" (2FA) in the coming months
        - 2FA is a second step in authenticating you as a user in Electio*Net* for security purposes.
        - We will send out instructions when the process begins.
2. Uncheck all **2018** UOCAVA voters – Generate a UOCAVA list
        - See Electio*Net* -> Help -> Instructions -> UOCAVA Check & Uncheck Instructions 2019
3. Add all new **2019** UOCAVA voters as you receive them without delay.

Thank You,
HAVA Office
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack on behalf of NHVotes
To: NHVotes
Subject: New Request for Access (RAE) Forms and Uncheck 2018 UOCAVA Voters
Date: Thursday, March 07, 2019 10:22:06 AM

Dear Clerks and Supervisors:

1. Every user in Election*Net* must fill out a new "Request for Access" (RAE) form – See attachment
    - Deadline to return the form is the end of March
        - Please give the completed form to your Town/City Clerk
        - Clerks return the completed form by scanning or faxing to: nhvotes@sos.nh.gov or 271-8242
    - We will be transitioning to "Two Factor Authentication" (2FA) in the coming months
        - 2FA is a second step in authenticating you as a user in Election*Net* for security purposes.
        - We will send out instructions when the process begins.
2. Uncheck all **2018** UOCAVA voters – Generate a UOCAVA list
        - See Election*Net* -> Help -> Instructions -> UOCAVA Check & Uncheck Instructions 2019
3. Add all new **2019** UOCAVA voters as you receive them without delay.

Thank You,
HAVA Office
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

REQUEST FOR APPLICATIONS

Policy Academy on Election Cybersecurity

IMPORTANT INFORMATION

Purpose: To maximize public confidence in elections by reducing technical risks to election systems and improving coordination between election officials and state cybersecurity leaders in the executive branch.

Opportunities Provided: Teams from five (5) competitively selected states will convene stakeholder workshops within their states to identify, refine, and/or implement promising practices in cybersecurity operations and communications directly related to elections.

Proposals Due:	8:00 PM ET, May 10, 2019
Informational Calls:	3:00 PM ET, April 5, 2019 2:00 PM ET, April 18, 2019 Conference Number: 888-858-6021 Conference Code: 202-624-5356
Selection Announcement:	Week of May 27, 2019
Project Period:	June 1, 2019 – December 1, 2019
Eligibility:	All eligible states, commonwealths, and territories.
NGA Contacts:	Maggie Brunner, Program Director, Cybersecurity and Communications, Homeland Security & Public Safety Division (202) 624-5364 or mbrunner@nga.org David Forscey, Senior Policy Analyst, Homeland Security & Public Safety Division (202) 624-5356 or dforscey@nga.org

PURPOSE

Election cybersecurity is a complex, long-term challenge that demands coordination across state and local governments. The National Governors Association Center for Best Practices (NGA Center)—in conjunction with technical support from the University of Southern California (USC)—is launching the *Policy Academy on Election Cybersecurity*, designed to facilitate intrastate dialogue and planning between election officials, governors' offices, and state cabinet agencies. This project will offer technical assistance to five states that have committed to improving intrastate coordination around election cybersecurity practices, policy, and planning. Combining expertise in state policy and technical research, the NGA Center will help interested states enhance interagency communication and cooperation, promote engagement by governors' offices, and

Application Checklist on Final Page

facilitate the development of statewide response plans for attacks on election infrastructure. Technical assistance offerings include facilitated strategic planning, policy design and development, state comparative analysis, document drafting, access to subject matter experts, and general capacity building.

Supporting organizations for the Policy Academy on Election Cybersecurity *include the National Association of State Election Directors and the National Association of Secretaries of State. Funding is provided by the Democracy Fund.*

BACKGROUND

Election officials have worked diligently against malicious attempts to undermine public trust in elections. Well before the 2016 elections, these efforts included important steps to address security vulnerabilities in voting systems, election management systems, and the procedures that rely on those systems.

Since 2016, the elections community has devoted unprecedented time, attention, and funding into cybersecurity controls designed to reduce risk. Driving these concerted efforts is evidence that foreign governments possess the means and intent to influence elections in the United States.

Notwithstanding geopolitics, other developments further underscore the need to prioritize election cybersecurity. First, in recent years, highly sophisticated hacking tools have become widely available, empowering novice attackers. Second, media reports have increased public concern about the security of elections and even highlighted opportunities for election interference. Third, increased public reliance on social networks for information magnifies the risks posed by isolated security events. For example, a single incident, real or perceived, affecting one voting or election system in one jurisdiction—reported by news media and amplified through social media—could undermine public confidence in broader election outcomes. In short, election practitioners confront a long-term struggle against a diverse set of potential attackers, who are increasingly capable, with a range of motivations, and who cannot all be deterred with the same tools.

Addressing this threat demands a whole-of-government approach that integrates all relevant cybersecurity resources and planning. This requires coordination across independent agencies. In many states, elections are managed by an independently elected constitutional officer who does not report to the governor. Yet significant cybersecurity expertise and resources can be found in departments and agencies subordinate to the governor. State information technology, homeland security, and public safety departments have expertise and capabilities that can boost the capacity of election officials to defend voting systems and election systems. Many National Guard cyber units comprise experts who work full-time in world-class technology companies. In dozens of states, cybersecurity leaders under the governor are collaborating through formal and informal governance bodies to write statewide cybersecurity strategies and disruption response plans that will guide cybersecurity investment and assistance.

A series of obstacles are limiting coordination between the election community and governors' cybersecurity leaders. Although the 2016 elections advanced a dialogue between election officials and governors' advisors, decades of siloed operations have deprived all stakeholders of the personal relationships and mutual understanding that are critical for long-term collaboration. Election officials are often left out of statewide strategies and plans. Election offices seeking help from the National Guard may lack support from the governors' office to request Guard resources. Governors' offices and state cabinet leaders may not always know what election officials need, from funding and technical assistance to coordinated public messaging.

POLICY ACADEMY DESCRIPTION

In recognition of the above challenges, the NGA Center, in a partnership with the University of Southern California, is launching the *Policy Academy on Election Cybersecurity*. This initiative is designed to help states maximize public confidence by fostering long-term coordination between election officials, governors' offices, and state cybersecurity leaders.

An NGA policy academy is a highly collaborative, team-based process for helping a select number of states develop and implement action plans that address complex public policy challenges. Participating states receive guidance and technical assistance (e.g., facilitated workshops, policy research, written products) from NGA Center staff and, as appropriate, access to subject matter experts from the private sector, research organizations, academia, and the federal government. A policy academy provides a forcing mechanism that focuses the time and attention of stakeholder groups that can prove difficult to convene under normal circumstances. The strategies and policies developed by participating states are intended to catalyze wider adoption of promising practices across the United States. The *Policy Academy on Election Cybersecurity* will benefit from direct research support provided by staff and faculty from the University of Southern California. ***Note: This project is not an academic study, and no state-specific findings or conclusions will be published or otherwise shared or discussed publicly without the express consent of participating states and other relevant stakeholders.***

Key Benefits

The primary activities of the *Policy Academy on Election Cybersecurity* include (a) technical assistance provided by NGA Center staff and appropriate subject matter experts; (b) a two-day multidisciplinary, in-state workshop to convene election officials and state cybersecurity leaders to create action plans; and (c) limited funding to cover travel costs for stakeholders. These activities will support goals that states choose to prioritize. Examples of appropriate state goals include:

- Integrating the needs of election officials into statewide strategies and investment plans;
- Engaging new gubernatorial administrations and building support for past and future election cybersecurity initiatives;
- Identifying and/or communicating election cybersecurity needs, corresponding budgets, and legislative strategies;
- Creating election cybersecurity priorities, policies, and plans for National Guard units;
- Leveraging all existing state, federal and/or local resources to scale training and assistance for local election offices (e.g., shared services contracts);
- Creating a statewide communications strategy that coordinates election cybersecurity messaging across relevant state and local offices;
- Integrating election offices with state fusion centers or security operations centers, or establishing a dedicated center for election cybersecurity activities;
- Identifying gaps in state law and potential solutions;
- Facilitating conversations with critical infrastructure owners and operators (e.g., internet service providers or utilities).

Application Checklist on Final Page

State Team Responsibilities

The Policy Academy will require preparation from state attendees before the in-state workshop, active team participation throughout the policy academy process, and a strong commitment to implementing action plans. Specifically, participating states are required to:

- *Participate in scheduled conference calls.* Following state selection, the NGA Center will host conference calls with participating states to orient them to the Policy Academy and outline next steps, including policy academy preparatory work and meetings, available technical assistance and resources from NGA Center staff and other experts, and site visits by NGA Center staff. Monthly conference calls will maintain coordination until the in-state workshop. Conference calls may continue on an as-needed basis for states who request additional virtual technical assistance following the workshop.
- *Develop state needs assessment and gap analysis.* Through initial conferences calls and other preparatory work, the NGA Center will complete a confidential gap analysis and needs assessment for each state. The gap analysis and needs assessment will provide team members with a better understanding of their state's challenges and serve as a baseline for evaluating outcomes of the policy academy.
- *Convene an in-state workshop.* The in-state workshop provides the core benefit of the Policy Academy process. Staff from the NGA Center will conduct a two-day visit in each state to help teams identify and/or implement action plans to achieve the objectives outlined in the Policy Academy application. Active participation by the entire Policy Academy team is required.
- *Complete evaluation survey and lessons learned report.* After the Policy Academy, participating states will be asked to complete a survey for the NGA Center on the work they accomplished during the project. State responses will be used for evaluation purposes and, with the state's consent, will be included in a public report on the lessons learned during the Policy Academy, to be disseminated to all other states and territories.

POLICY ACADEMY APPLICATION PROCESS

(SEE APPLICATION CHECKLIST ON LAST PAGE)

Step 1: Secure Commitment from the Governor and Chief Election Official(s)

The goal of this Policy Academy is to improve intrastate coordination between governors' offices, state cabinet agencies, and election offices. Interested state teams should secure approval from the governor and the chief election official of the same state. Each team will be asked to submit a joint letter or separate letters of commitment from the governor and chief election official. (See Step 3.)

Step 2: Identify a Policy Academy Team

Each interested state should assemble a high-level multidisciplinary "core" team of state representatives, plus a larger, more comprehensive team. The core team will (a) manage the full team; (b) prioritize state objectives; and (c) lead coordination with the NGA Center and other relevant support organizations.

Team leads: The core team will be led by two state officials, one selected by the governor's office, and one selected by the chief state election official(s) (or by the designee of the chief state election official).

Application Checklist on Final Page

Core team: The team leads will designate the rest of the core team, comprising a mix of relevant representatives from each respective branch of government. The core team must include a minimum of six (6) state officials, including the team leads; each state is free to determine the appropriate size of its core team beyond the minimum. Two possible examples of core teams are:

- Example 1: Adjutant General, statewide Chief Information Officer, statewide Homeland Security Advisor, Secretary of State, Election Director, and Chief Information Officer for the statewide election office.
- Example 2: Head of the Department of Motor Vehicles, statewide Chief Information Security Officer, Commissioner of Public Safety, two county Election Directors, and the statewide Elections Commissioner.

Full team: The core team will designate a larger team that can include not only state officials, but also non-state and local actors, such as local election officials, academic advisors, nonprofit representatives, and others. *The full team does not need to be described in the written application.*

Step 3: Draft the Application Narrative. Formal applications to participate in the Policy Academy cannot exceed six (6) pages and must include:

(1) *Letter(s) of application from the governor and the chief election official:* The letter or letters of application, co-signed by the governor and chief election official (or, if using separate letters, signed by each), should briefly articulate the state's interest in and desired outcomes related to this project, and how those outcomes fit within the state's commitment to election security. The letter(s) must designate the two team leads who will direct the team's efforts with the NGA Center. The letter(s) will *not* count against the six-page limit.

(2) *Proposal narrative:* The proposal narrative should not exceed six-pages single-spaced, 11-point font, 1" margins. **Please see the final page of this document for evaluation criteria that offer a guide for narrative content**.

Step 4: Submit the Application. All proposals must be received by **5:00 PM PST on May 10, 2019**. Only one application per state will be considered, and it must be transmitted by a state employee. Prior to submission, please assemble the proposal materials into a single PDF document. **Please email the proposal to Maggie Brunner at mbrunner@nga.org.** NGA will confirm receipt within one business day.

POLICY ACADEMY TIMELINE

The following is a tentative schedule for the academy:

3:00 PM ET, April 5, 2019 Number: 888-858-6021 Code: 202-624-5356	**1st Bidders' Call** The NGA Center will host an optional conference call for all interested states to answer questions about the Request for Application (RFA) process, proposal content, submission requirements, or other issues.
2:00 PM ET, April 18, 2019 Number: 888-858-6021 Code: 202-624-5356	**2nd Bidders' Call**

Application Checklist on Final Page

	The NGA Center will host an optional conference call for all interested states to answer questions about the RFA process, proposal content, submission requirements, or other issues.
5:00 PM PST, May 10, 2019	**Proposals Due**
Week of May 27, 2019	**State Selection Announcement** The NGA Center will notify states of their application status and issue a press release announcing winning states.
June 2019 – December 2019	**In-State Workshops** Objectives: • Engage state team in planning process • Refine initial recommendations • Develop strategic action plan for implementing recommendations
Ongoing	Monthly conference calls and webinars with Policy Academy staff and other participating states.

SELECTION CRITERIA **(Total points possible = 100 pts)**

Note: States can use these criteria in drafting the narrative portion of their application.

Category	Description	Value
Description of the Problem	• Applicants should describe current efforts to secure election and voting infrastructure at the state and local levels. • Applicants should explain limitations of the state's current approach that may be relevant.	20 points
Anticipated Benefits and Potential Outcomes	• Applicants should explain how improving coordination between election offices and other state cybersecurity offices will help the state address identified challenges and improve their overall efforts to secure elections. They should articulate a clear "business case" for how proposed changes will help them achieve state goals. • Applicants must demonstrate that the state is poised to make significant progress toward improving their statewide efforts to secure election infrastructure. For example, is there buy-in from key political leaders, agency leadership, local government, and communities? If not, will the Policy Academy help to solve that? • Applicants should identify specific outcomes they hope to achieve by the end of the Policy Academy. *Applicants should focus on activities that support election cybersecurity. This Policy Academy will not focus on information operations.*	30 points
Obstacles to Implementing Solutions	***This section does not count toward the six-page limit.***	20 points

Application Checklist on Final Page

	• Applicants should identify any potential obstacles that could derail development or implementation of their goals. Further, they should explain how they might address those challenges. *For states that are undergoing a gubernatorial or chief election official transition, please address how you will pursue completion of Policy Academy goals and activities through that transition.*	
Evaluation Plan	• Applicants must identify a plan that ties goals and objectives to tangible metrics. • Describe what those metrics are and how they would be measured. ***This section does not count toward the six-page limit.***	10 points

Team Composition and Member Roles	***This section does not count toward the six-page limit.***
	
	• **Team Leads**: The governor and chief election official must each designate a separate representative from their branch to co-lead the state's Policy Academy project.
	• **Core Team**: Each state must assemble a multi-disciplinary "core" team comprising of a minimum of six (6) state leaders (including the team leads) with demonstrated equities in elections, cybersecurity, homeland security, and/or emergency preparedness. Applicants should briefly discuss the rationale behind the core team composition and the roles and responsibilities each member will take on in support of achieving team objectives.
	  ○ Please provide each core team member's name, title, work address, phone, and e-mail address.
	  ○ *Note: resumes or curriculum vitae are not required.*
	• **Full Team:** States can identify additional members of the full team, above and beyond the core team. This can be a much broader and more diverse group, and can include state, local, and non-governmental partners, to consult with during the Policy Academy and to convene during the state's two-day workshop.
	  ○ Note: For purposes of the full team members, simply listing agencies/affiliations, rather than specific individuals, is sufficient.
	
	This section does not count toward the six-page limit.
		20 points

Disclaimers

This request for application is not binding on the NGA Center, nor does it constitute a contractual offer. Without limiting the foregoing, the NGA Center reserves the right, in its sole discretion, to reject any or all applications; to modify, supplement, or cancel the RFA; to waive any deviation from the RFA; to negotiate regarding any application; and to negotiate final terms and conditions that may differ from those stated in the RFA. Under no circumstances shall NGA Center be liable for any costs incurred by any person in connection with the preparation and submission of a response to this RFA.

Application Checklist on Final Page

Policy Academy on Election Cybersecurity
Application Checklist

Application Process

- ☐ Consult with Governor's Office and Chief Election Official Regarding Application Process
- ☐ Identify Team Leads
- ☐ Identify Core Team
- ☐ Prepare Narrative Description (maximum of six (6) pages single-spaced)
- ☐ Email Application in PDF Format to Maggie Brunner at mbrunner@nga.org **before 5:00 PM PST on May 10, 2019**.

Application Contents

- ☐ Letter(s) of Application from Governor and Chief Election Official
- ☐ Narrative Description (Maximum length of six (6) pages, single-spaced)
  - Description of the Problem
  - Anticipated Benefits and Potential Outcomes
  - Obstacles to Implementing Solutions
  - Evaluation Plan (does not count toward the page limit)
  - Team Composition (does not count toward the page limit)
    - Team Leads
    - Core Team
    - Full Team (optional—members of the full team can be identified after the Policy Academy application has been submitted)

From: Colleen McCormack
To: Bhanu Pothugunta
Subject: NH ElectioNet - 2FA
Date: Wednesday, January 16, 2019 1:36:54 PM

Bhanu,

We just refreshed UAT with the Production data yesterday morning.

In this refresh, we lost a step in the 2FA process.

I enabled everyone for the 2FA in the office. I had to add all of the mobile phone numbers and emails once again, since it was not Production.

Each one of us, was allowed to log in with only our password. We did not receive the "verification" screen.

Can you look into this for me?

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

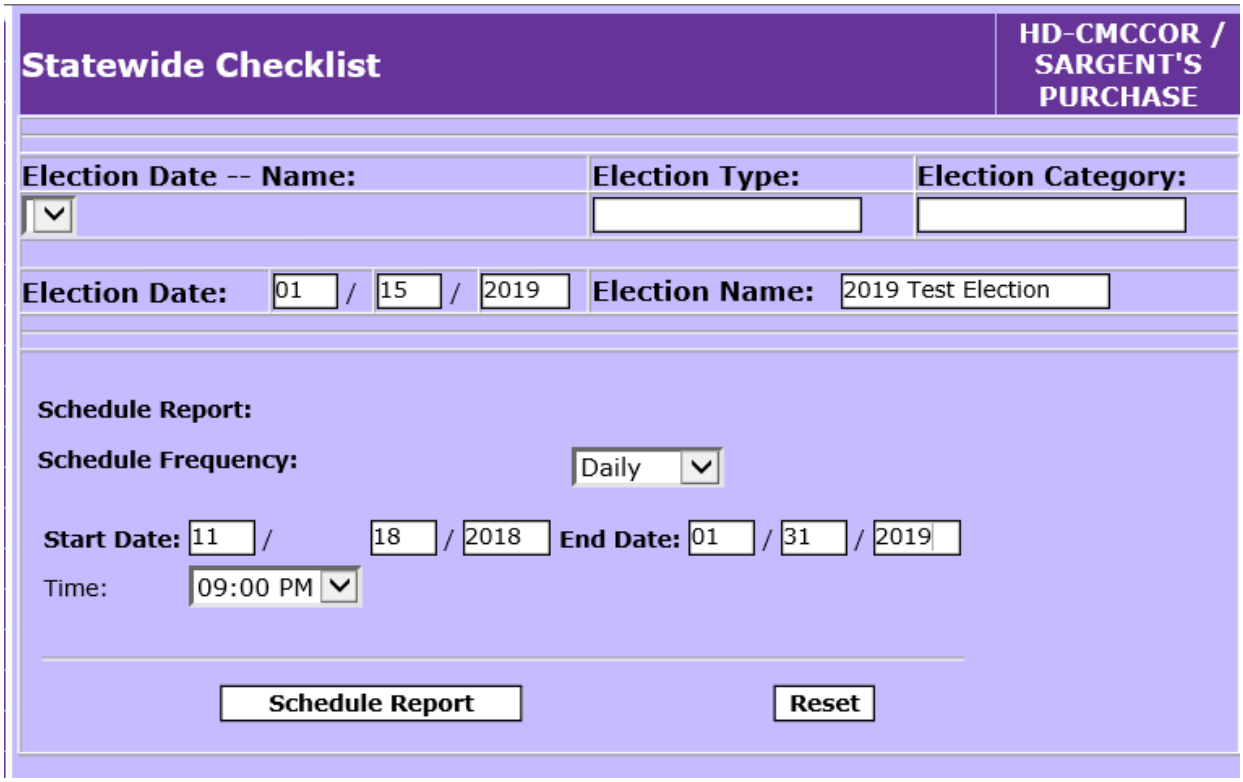
From: Colleen McCormack
To: Bhanu Pothugunta
Subject: NH ElectioNet - Statewide Checklist
Date: Friday, November 16, 2018 11:53:50 AM
Attachments: image001.png

Bhanu,

The statewide report ran in production this morning.

I will change the scheduled end date to 2019. Can you monitor this for me?

I will be out all of next week. Have a good Thanksgiving.



Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: NHVotes@sos.nh.gov
To: Colleen McCormack
Subject: NH SVRS Authentication Code
Date: Thursday, April 25, 2019 4:34:56 PM

Dear BHANU POTHUGUNTA,

You are receiving this email because an authentication request was submitted in the NH SVRS. Enter the authentication code that appears below to verify your account.

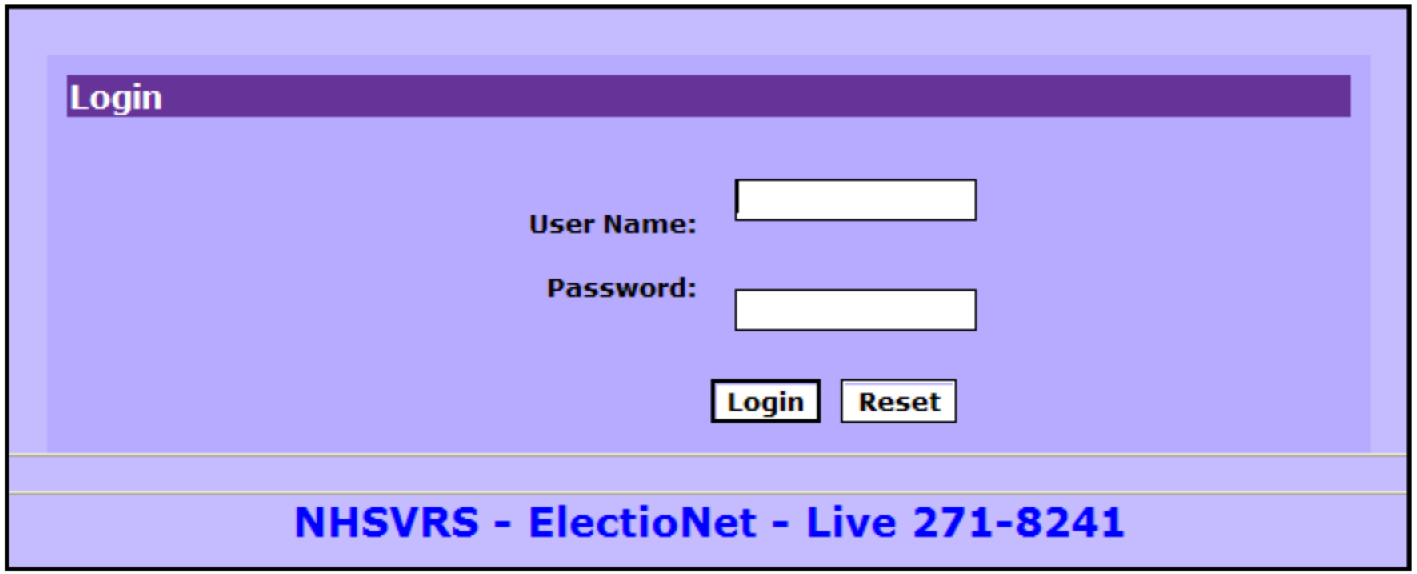
The authentication code is: [redacted]

Do not forward or give this code to anyone. If you did not initiate an authentication request, contact the ElectioNet help desk to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Introduction to ElectioNet

Welcome to New Hampshire Statewide Voter Registration System - ElectioNet



Introduction Agenda

- ✓ Confidentiality, Security, Computer Tips,
- ✓ Passwords User Names & Login, Navigation and Terms
- ✓ Show Reminder Screen: Voters that have Moved Out,
  "SESSIONS" Pending Approval/Removal
  NHVRIN Death Records
- ✓ Inquiries: Searching, Looking at Voter Info., Print Reg. Form
- ✓ Voter Registration Forms, Absentee Ballots, UOCAVA/FPCA
- ✓ Inquiry Searches, Entering in a New Voter
- ✓ Elections & Reports: Alpha, Checklist, CVA, OOS DL, Affidavits

002522

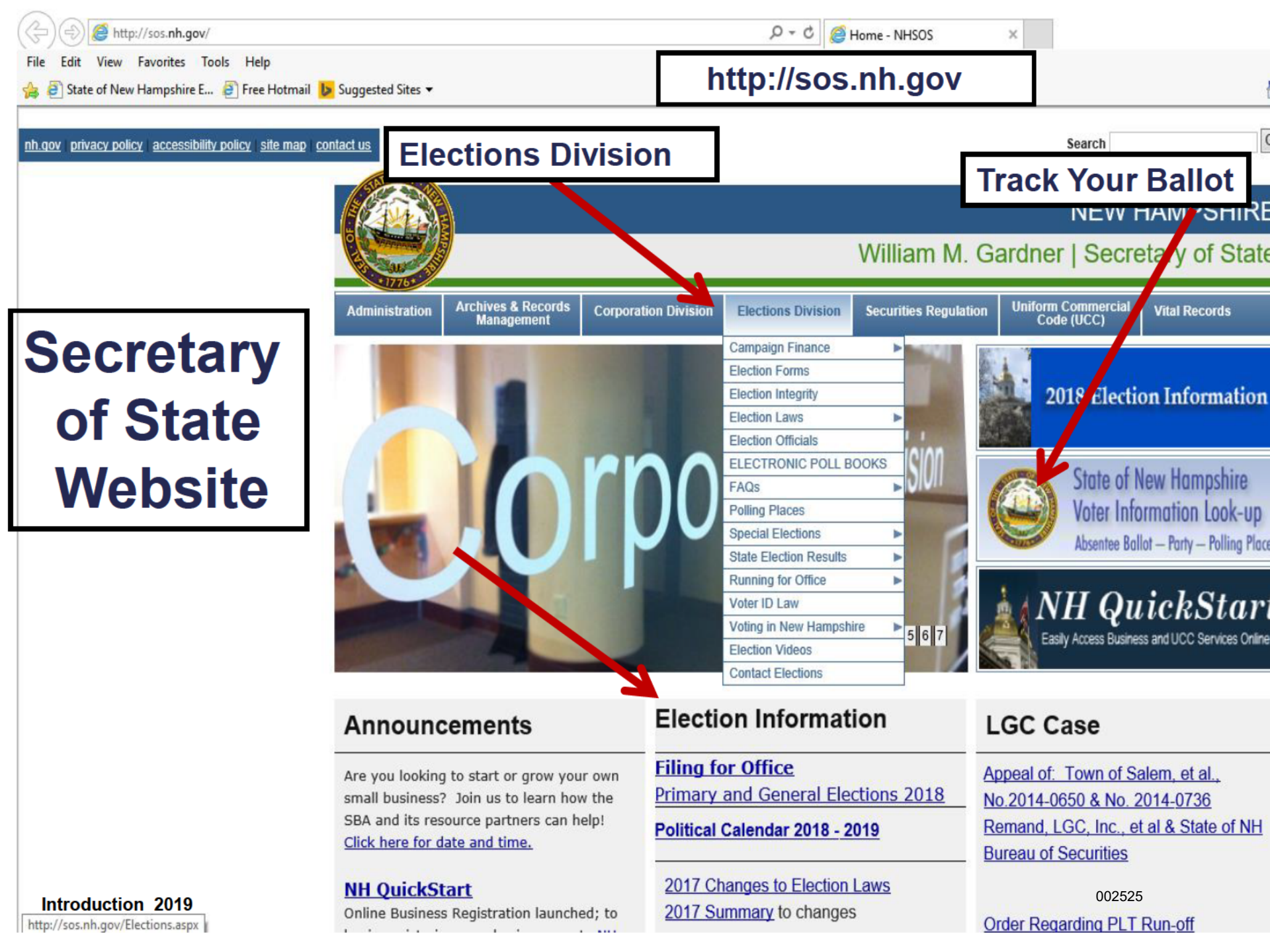
Introduction to ElectioNet

Moe's 12" Submarine Sandwiches
Cut into 3 pieces

- Original – Italian
- Tuna
- Turkey
- Roast Beef
- Veggie

002523


LET'S
TAKE
A
LOOK
AT
YOUR
TRAINING
HANDOUT
MATERIALS
002524


http://sos.nh.gov/
Home - NHSOS
File Edit View Favorites Tools Help
State of New Hampshire E... Free Hotmail Suggested Sites
http://sos.nh.gov
nh.gov | privacy policy | accessibility policy | site map | contact us
Search
Elections Division
Track Your Ballot
Secretary of State Website
William M. Gardner | Secretary of State
Administration
Archives & Records Management
Corporation Division
Elections Division
Securities Regulation
Uniform Commercial Code (UCC)
Vital Records
Campaign Finance
Election Forms
Election Integrity
Election Laws
Election Officials
ELECTRONIC POLL BOOKS
FAQs
Polling Places
Special Elections
State Election Results
Running for Office
Voter ID Law
Voting in New Hampshire
Election Videos
Contact Elections
2018 Election Information
State of New Hampshire
Voter Information Look-up
Absentee Ballot – Party – Polling Place
NH QuickStart
Easily Access Business and UCC Services Online
Announcements
Are you looking to start or grow your own small business? Join us to learn how the SBA and its resource partners can help!
Click here for date and time.
NH QuickStart
Online Business Registration launched; to
Election Information
Filing for Office
Primary and General Elections 2018
Political Calendar 2018 - 2019
2017 Changes to Election Laws
2017 Summary to changes
LGC Case
Appeal of: Town of Salem, et al., No.2014-0650 & No. 2014-0736 Remand, LGC, Inc., et al & State of NH Bureau of Securities
002525
Order Regarding PLT Run-off
Introduction 2019
http://sos.nh.gov/Elections.aspx

Introduction to ElectioNet

CONFIDENTIALITY AGREEMENT

The NH Voter Registration information we used to prepare this training program is *private and confidential*.

Course Voter Registration Information is not to be disclosed. All morning course materials and State law books may be taken home.

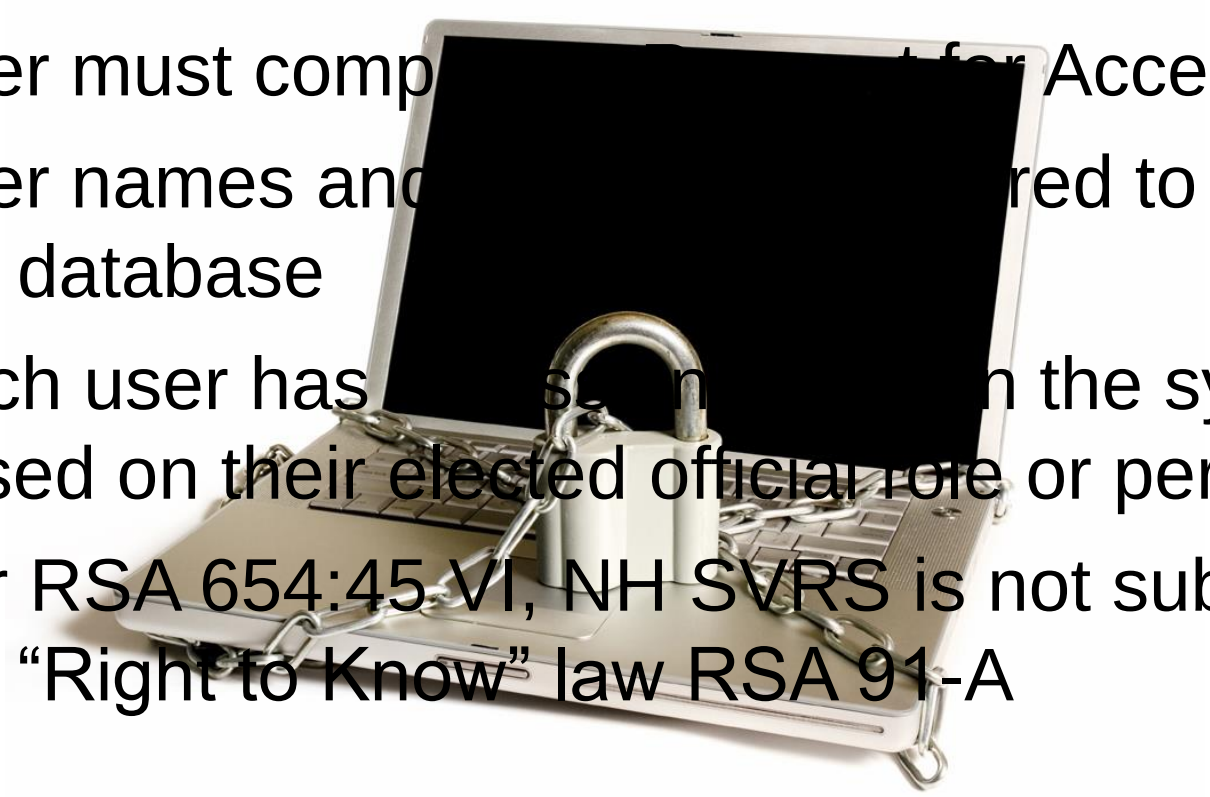
Afternoon materials must stay in the training room and may not be taken home.

002526

Introduction to ElectioNet

Security :

- Secure website “https”
- User must comp[illegible] Access Form
- User names and [illegible]red to log into the database
- Each user has [illegible] the system based on their elected official role or permission
- Per RSA 654:45 VI, NH SVRS is not subject to the “Right to Know” law RSA 91-A



002527

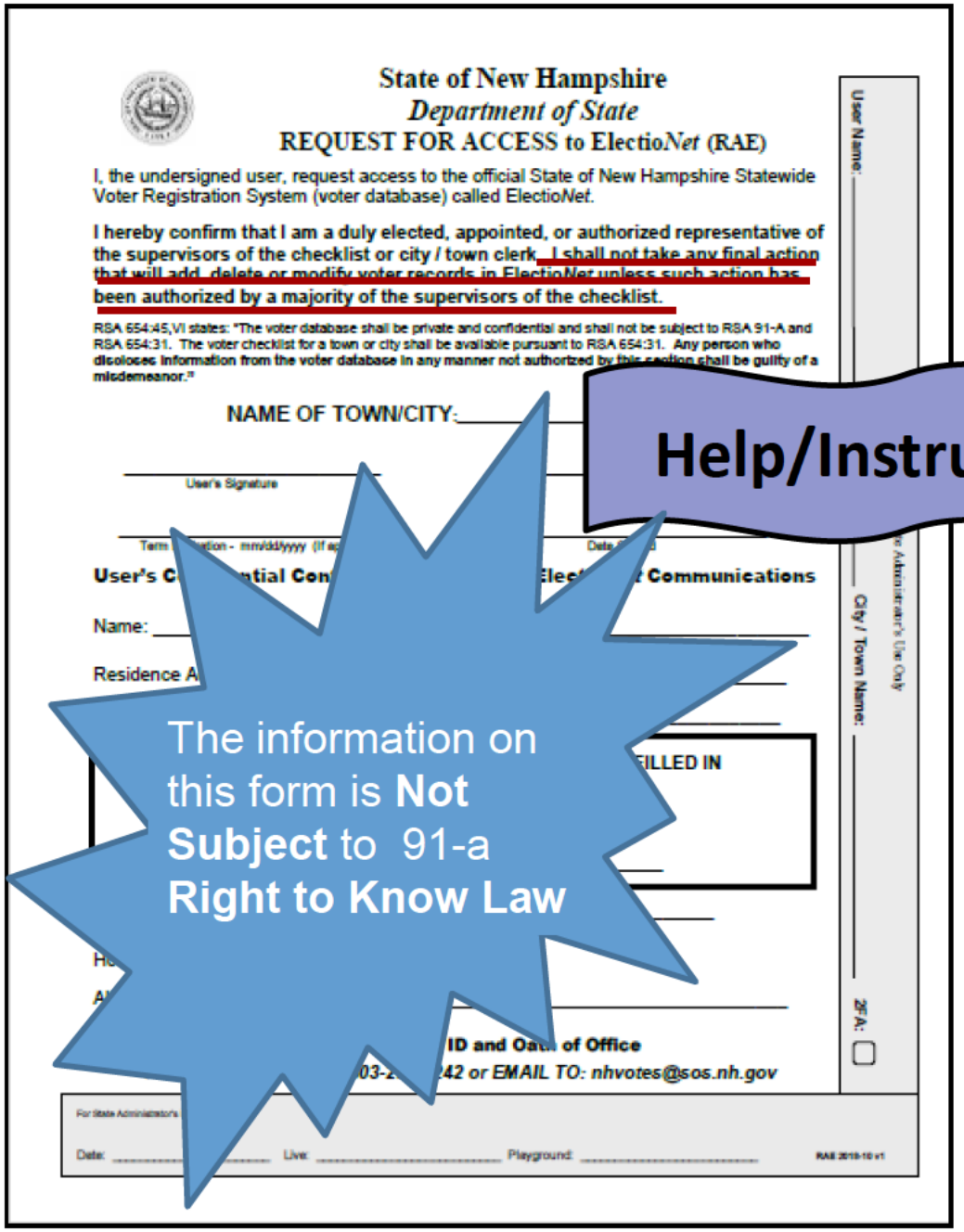
RAE Form

Every Election*Net* user must complete this form!

This is your "privacy statement" by signing.

Your e-mail address is used for Election*Net* and Election communications.

Each user should have their own email address.



Introduction to ElectioNet

Security - User Names :

- Up to 9 Characters in length
- Permanent
- Not case sensitive
- First letter of your first name followed by your last name. Ex: **jbrown**
- If more than one user with the same name in Electionet, a number is assigned, in numerical order, as the last character. Ex: **jbrown1**

Introduction to ElectioNet

Security - Passwords:

- Users create their own password after logging in with their temporary password
  - Write it down 
  - Secure the password 
- Passwords must be 6-8 Alpha-Numeric and should include “Special” Characters
- Special Characters: @ # $ % & * + =!:;><?~`{] ()
- Must contain at least 1 letter and 1 number

Introduction to ElectioNet

Security - Passwords:

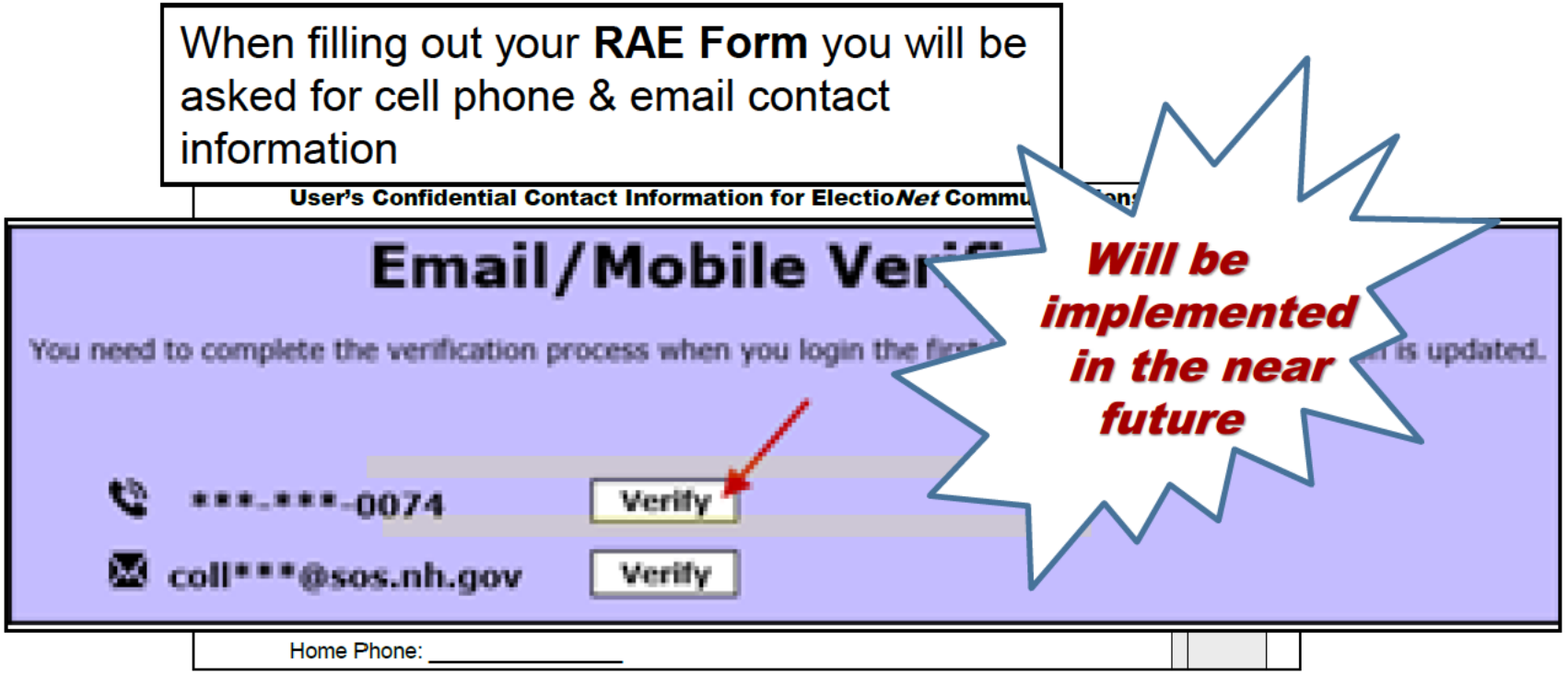
- Case Sensitive
- Expire every 90 Days
- Cannot re-use 8 of your last 9 passwords
- **Never share your password with anyone!**
- Don't make it simple enough for someone to guess

2FA-Two Factor Authentication

Extra Layer of Security

This new security feature authenticates your:
Email Address & Phone # to your Identity as a user in Election*Net*

When filling out your **RAE Form** you will be asked for cell phone & email contact information



002532

Introduction to ElectioNet

Security - Process and Procedures:

- End user is the last line of defense – keep passwords safe, secure and confidential.
- **Do not** allow ***anyone*** to use your computer using your login ID and password.
- Keep your Voters safe and secure – they are in your hands

Introduction to ElectioNet

Secure or Not Secure

002534

Chapter Review

If you become Locked Out of Electio*Net* how do you get back in?

Call the **ElectioNet HELP DESK – 603-271-8241**

What is the procedure if you changed your Email Address?

Fill out and send a new RAE Form to this office

What if my PASSWORD expires?

No matter how long it is after expiration you will be able to log in once and Change your PASSWORDto a new one

Why is it important not to let anyone work in the system using your Password?

Work is time and date stamped. If there is a problem you are accountable

Why must we be so security conscious?

Your responsibility is the secure handling of **personal/private information**

You are the **Last Line Of Defense**

002535

Introduction to ElectioNet

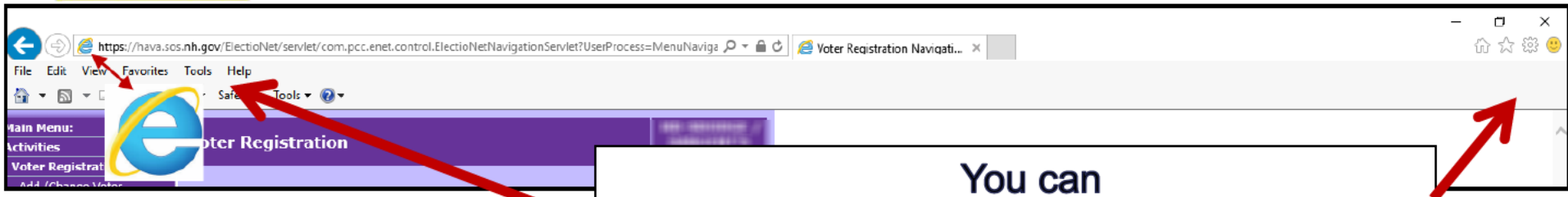
Browser Based Internet System

Internet Explorer Only

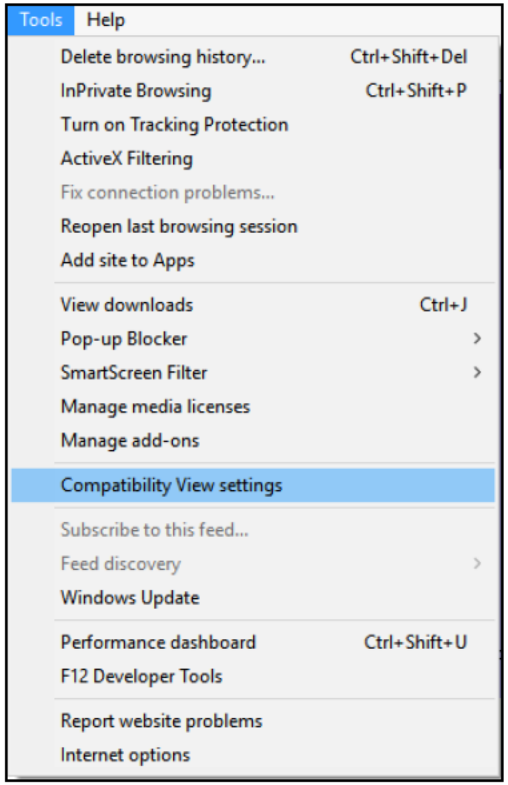
NOT Google Chrome, Safari, Firefox, Edge or any other browser

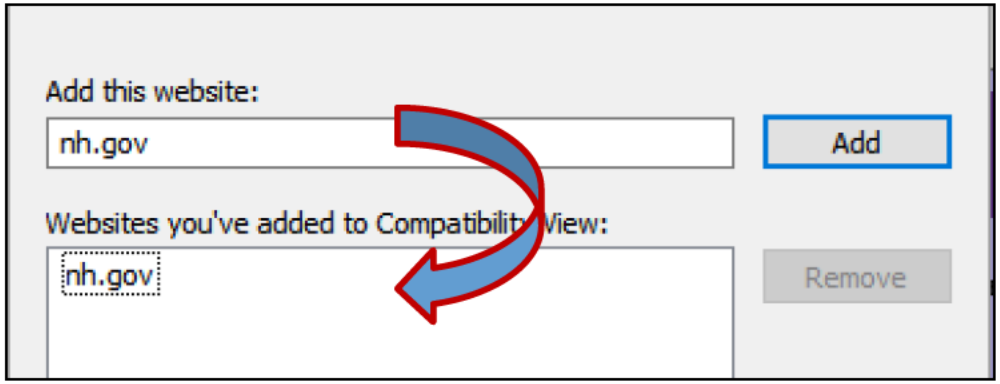
Not Compatible with Apple Computers

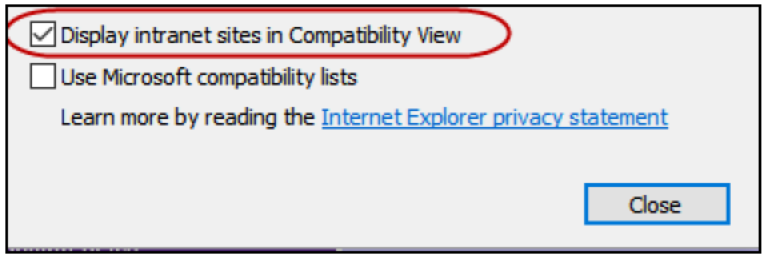
Introduction to ElectioNet



You can
Click Tools for **Compatibility View** issues or
hold the "ALT" key and the letter 'T' down

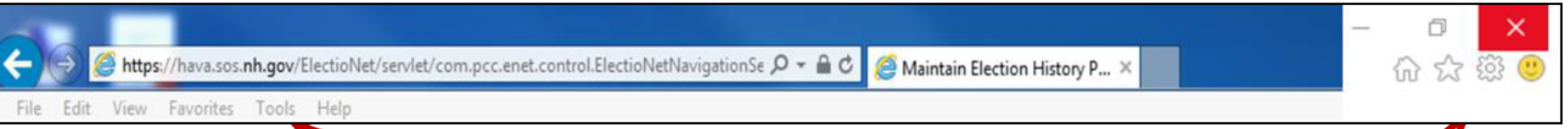




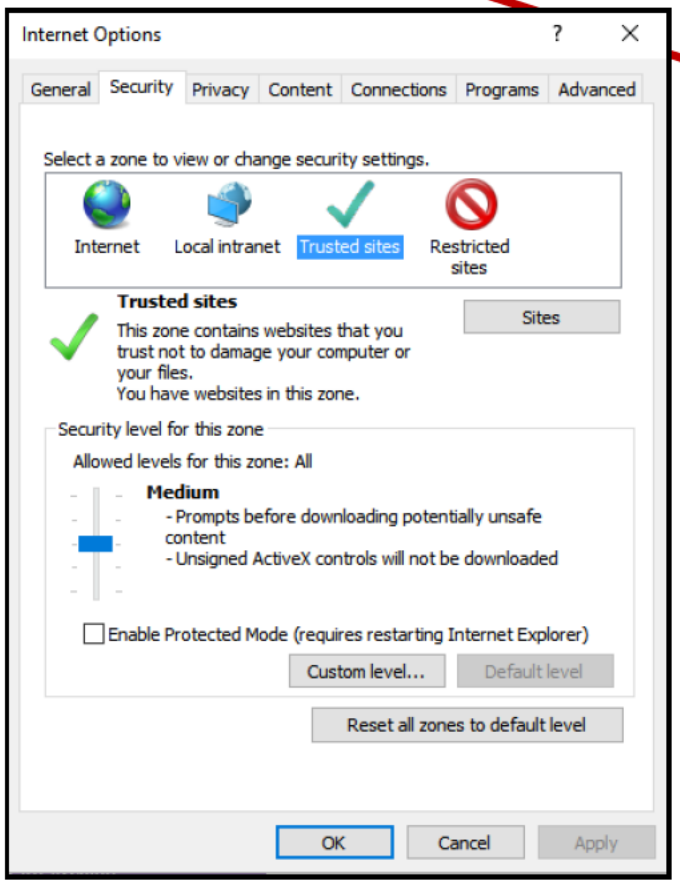


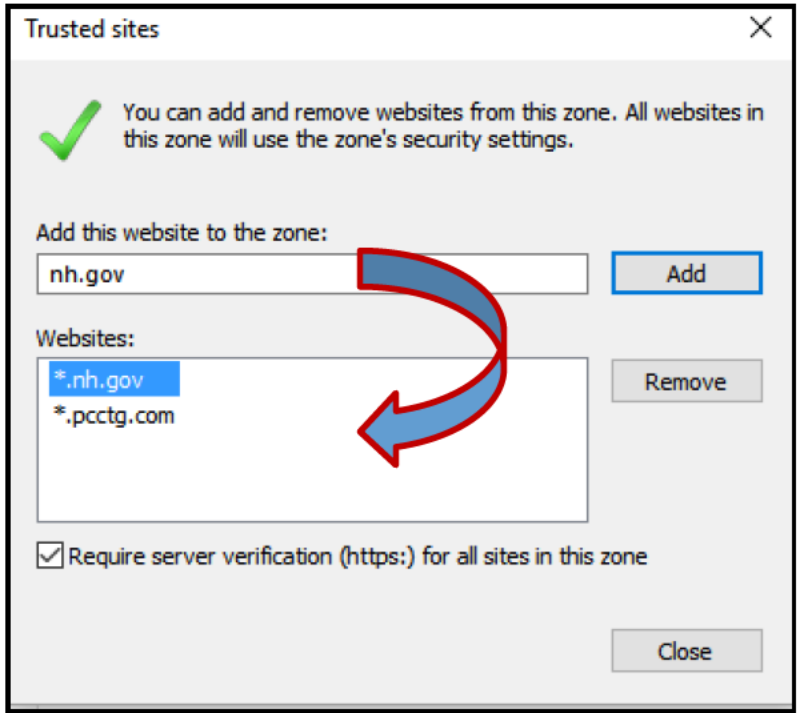
002537

Introduction to ElectioNet



ElectioNet must be a trusted website.
This can be found in
Tools / Internet Options





002538

Introduction to ElectioNet

URL Addresses for ElectioNet

ElectioNet Live - Work

https://hava.sos.nh.gov

ElectioNet Playground – Learn & Play

https://havauat.sos.nh.gov

002539

Chapter Review

What browser must you use when in Electio*Net*?

Internet Explorer **Only**

Why are there 2 websites for Electio*Net*?

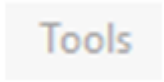
Playground is to get familiar with the program and try new things
Live site to do your work

What is an indication you need a Compatibility View setting update?

Popups do not respond correctly

Where do you find Trusted Site?

Tools>Security Tab>Trusted Site



002540

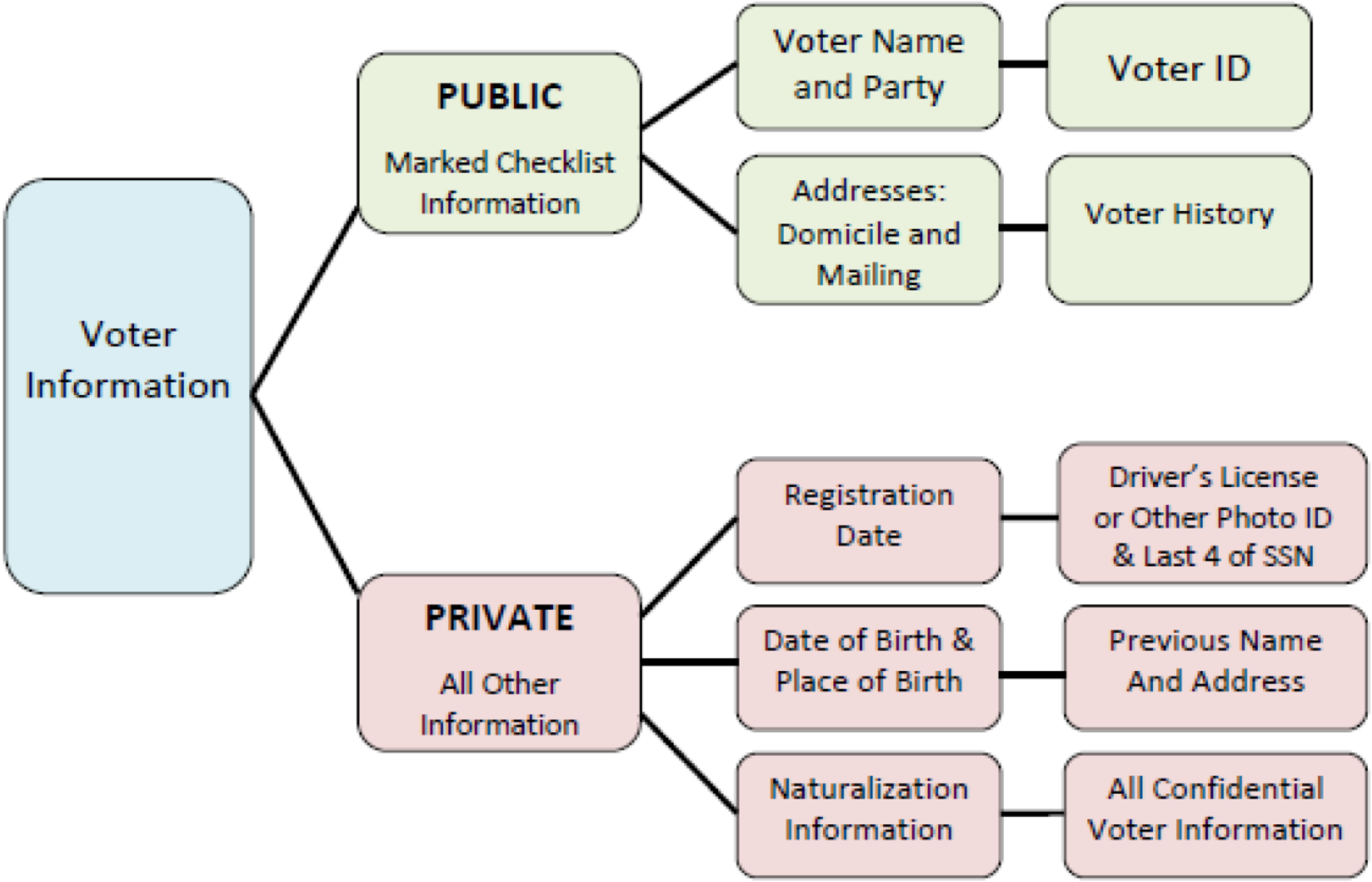
Introduction to ElectioNet

Public or Private?

VOTER

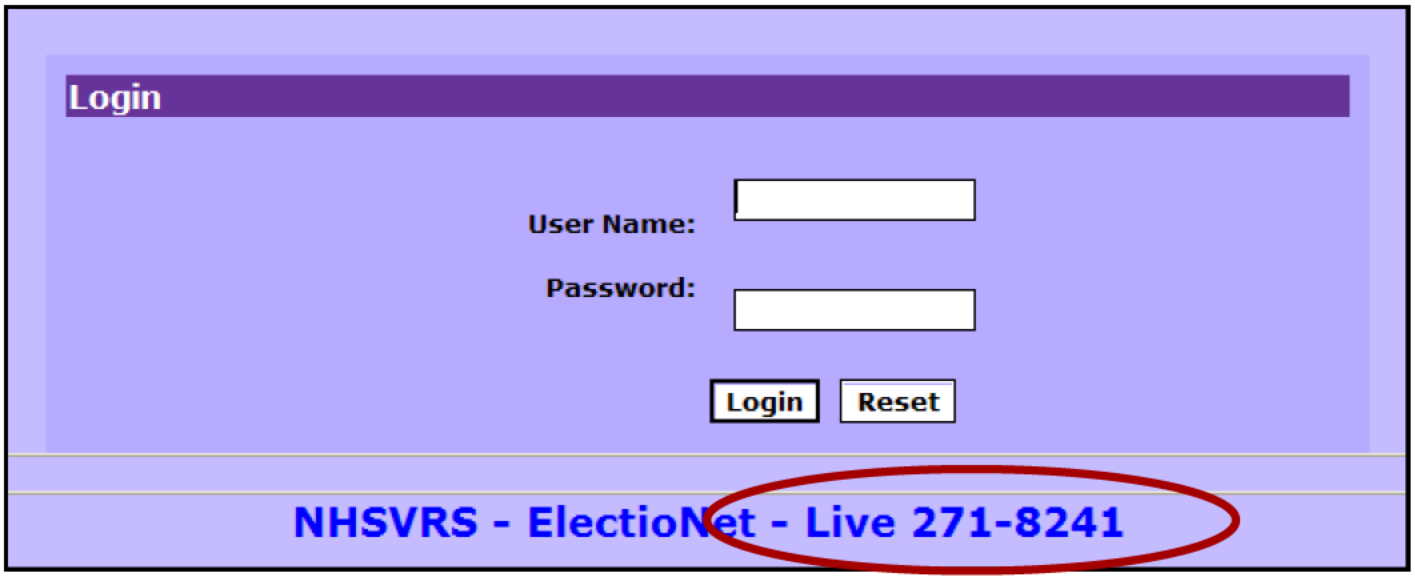
INFORMATON

Voter Information – Public or Private



Introduction to ElectioNet

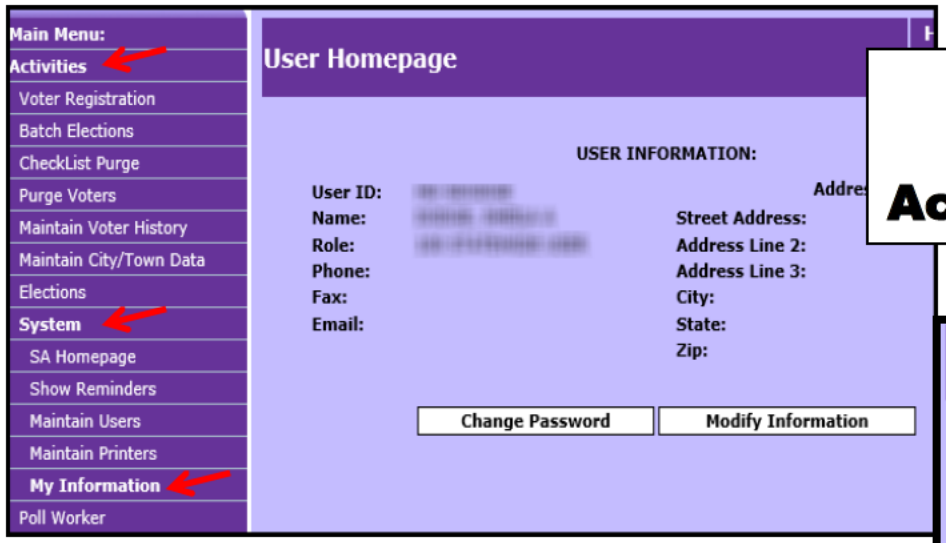
Log into ElectioNet



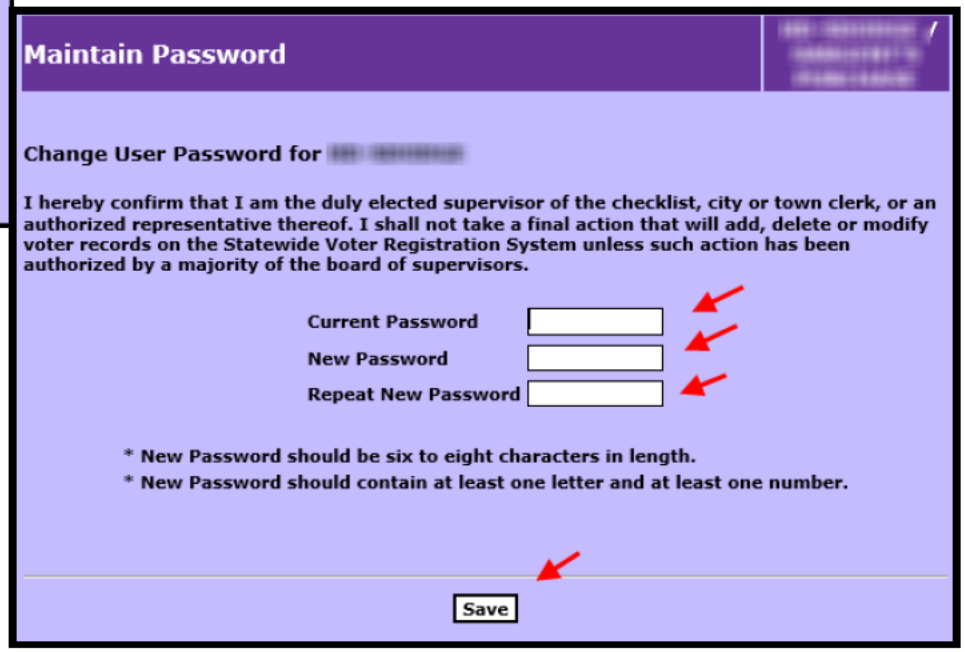
Introduction to ElectioNet

Log-In Screen Messages – User Information

Introduction to ElectioNet



You can change your Password at any time
Activities->System->My Information



Passwords expire in 90 days. After the 90 days you are able to log-in with the expired password and change it to a new password.

002545

Introduction to ElectioNet

Introduction to ElectioNet

Locked out of ElectioNet Procedure:
Call the ElectioNet Help Desk

Contact ElectioNet Help Desk
Email – nhvotes@sos.nh.gov
Phone – 1-800-540-5954
603-271-8241

The ElectioNet Help Desk will e-mail you a temporary password to your most current e-mail address on your signed **RAE** form.

Introduction to ElectioNet

Statewide Database Terms:

Status	
• Pending	Not on a checklist
• Active	**On a checklist**
• Pending Removal	**On a checklist**
• Removed	Not on a checklist
• Removed/Merged	Not on a checklist
• Incomplete	Not on a checklist
• Rejected	Not on a checklist

Introduction to ElectioNet

Statewide Database Terms:

- **Voter ID**
  - Unique 9 digit number for each voter
  - ID starting with 0-2 is a converted record
  - ID starting with 3 is a post-conversion record
- **Default Date of Birth**
  - 01/05/1776 – No DOB converted into the system
- **Default Date of Registration**
  - 01/05/1797 – No DOR converted into the system
- **Legacy ID**
  - Individual City/Town Voter ID# from their “old” system

Chapter Review

Can I change my User Name?

No your User Name never changes unless you become a user in another town

Where do I go to change my own Password?

Activities>System>My Information

Why is Status so important?

Status determines whether the Voter is on the Checklist or Not

Is a Voter in the Pending Removal Status on the Checklist?

Yes they have not been Approved for the Removal

A Voter ID# starting with a 3 indicates what?

The voter registered after 2006

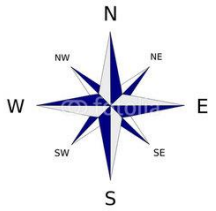
What is 2FA?

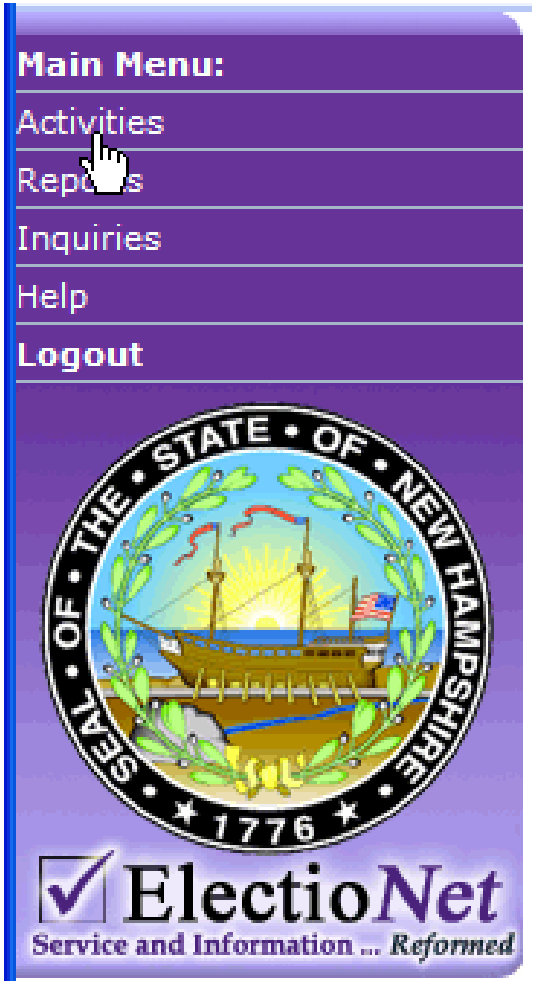
Two-factor Authentication – verifies user as an authorized Electio*Net* User

What would be Public Information about a voter

The information that is on a Marked Checklist – See Handout

Introduction to ElectioNet





Navigation:

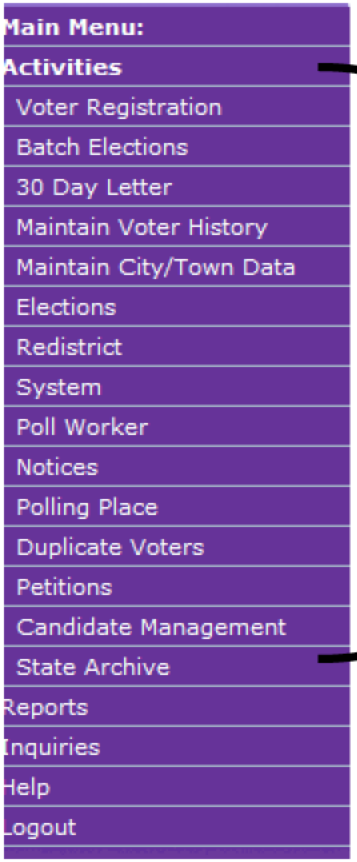
There are four headings under the Main Menu:

- Activities
- Reports
- Inquiries
- Help

002551

Introduction to ElectioNet

Navigation:



Clicking on any one of the 4 main headings will expand that section

Activities shown here expanded

Only one heading can be expanded at a time

002553

Introduction to ElectioNet

"LANDING PAGE"

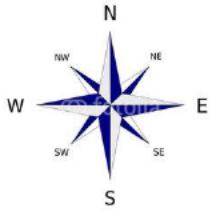
Reminders Screen: Your To Do List

Activities / System / Show Reminders

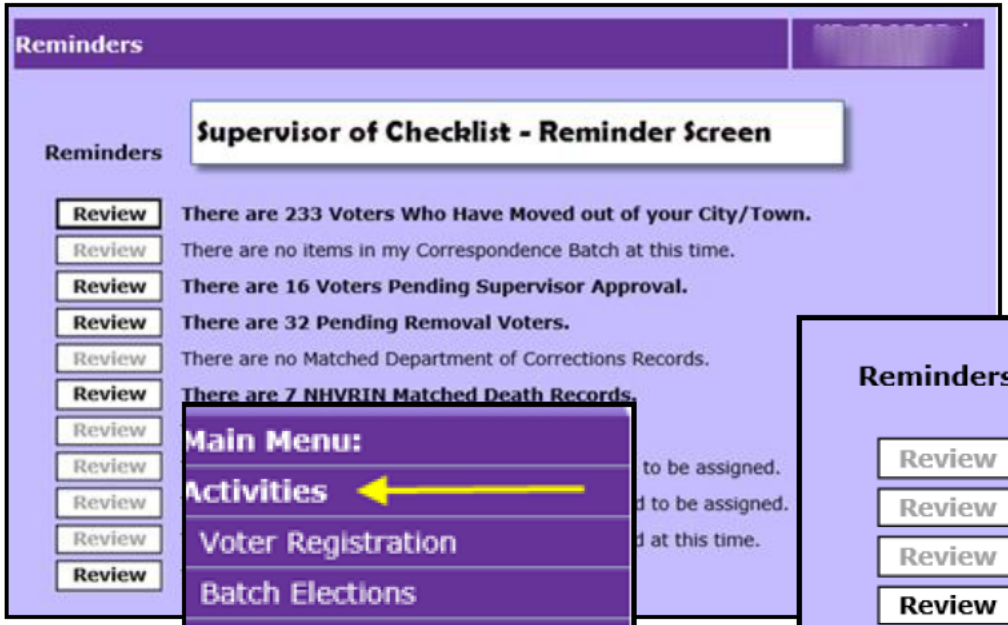
- The landing page when you log into Election*Net*
- Supervisor and Clerk reminder screens are not the same
- Informs Supervisors or Clerks of any voter records that need action taken to **add** or **remove** a voter from the checklist
  (requires a public session see page 1-3 in the EPM)
- Informs users if there is any correspondence to print

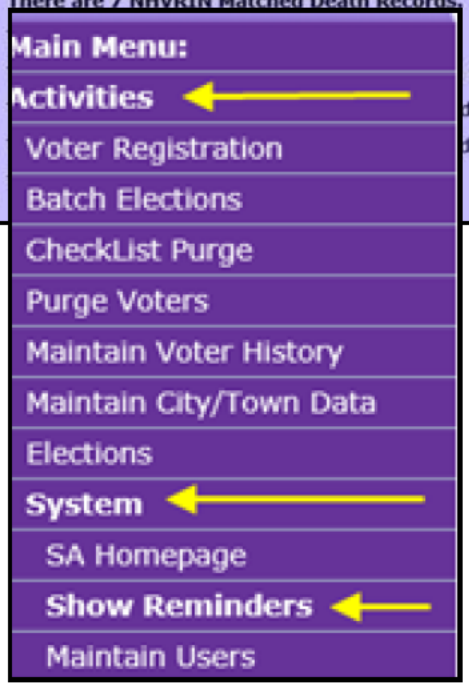
002554

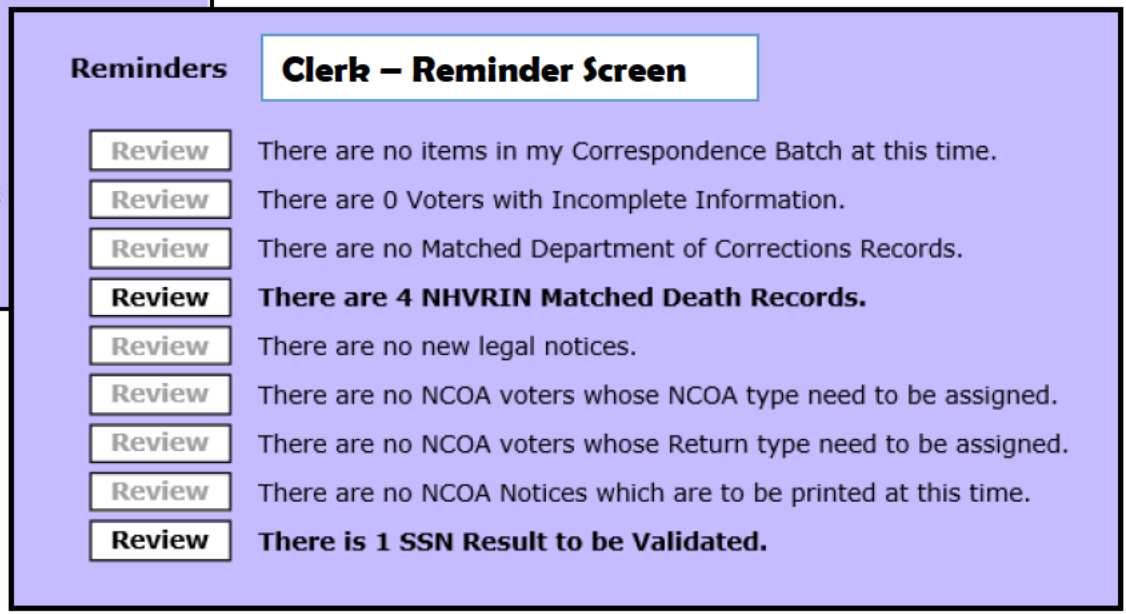
Introduction to ElectioNet



Supervisors and Town/City Clerks have different Reminder Screens

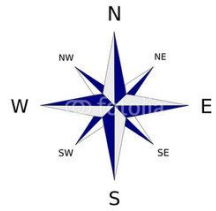






002555

Introduction to ElectioNet



Show Reminder Screen is your work to be done at your **Public Session**.

Data entry work should be done as it comes in (in a timely manner) prior to the Session so the **Pending Approvals** & **Removals** are there to act upon.

Any new work can be entered at the Session to act apon prior to adjournment.

In a Session just prior to an election it is especially important to have all work in the system and completed before you leave the meeting. RSA 654:27;RSA 659:13

There must be a quorum at your meeting.

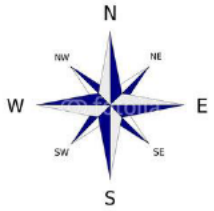
Data entry can be done at anytime & does not require a quorum.

Meeting Minutes are to be kept for your Sessions. Are Subject to 91-a Right to Know

Refer to the **EPM**, **Political Calendar** and **NH Election Laws book**

002556

Introduction to ElectioNe



Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
System
SA Homepage
Show Reminders
Maintain Users
Maintain Printers
My Information
Poll Worker
Notices
Polling Place
Duplicate Voters

Reminders

Landing Page when 1st logging in
Your "To Do" List

Click

Reminders

Review	**There are 8 Voters Who Have Moved out of your City/Town.**
Review	There are no items in my Correspondence Batch at this time.
Review	**There are 15 Voters Pending Supervisor Approval.**
Review	**There are 6 Pending Removal Voters.**
Review	There are no Matched Department of Corrections Records.
Review	**There are 15 NHVRIN Matched Death Records.**
Review	There are no new legal notices.
Review	There are no NCOA voters whose NCOA type need to be assigned.
Review	There are no NCOA voters whose Return type need to be assigned.
Review	There are no NCOA Notices which are to be printed at this time.
Review	There are no SSN Results to be Validated.

002557

Inquiry - Voters Moved Out of City/Town

HD-SDODGE / SANBORNTON

The following voters have registered to vote in another New Hampshire City/Town. These voters are no longer on your checklist.

Review and print the list of voters. Pull the paper voter registration from your "Active" file and put them in your "Inactive" file. Retention [illegible]A:3-a, requires you to retain these forms for 7 years from the date of removal.

NEW

Status means the Status of the record in your city/town at the time of registering in another city/town

Removed Status means the voter was removed by your city/ town prior to reregistering in another N.H. city/town

Voters Who Have Moved from your city/ town:

	Removal Date	Status	Name (Previous Name)			New Ward
☐	01/01/2019	Active	[redacted]			00
☐	11/06/2018	Active	[redacted]			00
☐	11/06/2018	Active	[redacted]		00	00
☐	11/06/2018	Active	[redacted]		00	00
☐	11/06/2018	Active	[redacted]			00
☐	11/06/2018	Active	[redacted]			08
☐	01/01/2019	Removed	[redacted]		00	00
☐	11/06/2018	Active	[redacted]		00	01

1

<< Go to Page No.

Select All | Print List | Print Labels | Approve Moved Voters

002558

Voters Move Out Of City/Town Process – Show Reminder Screen

02/23/2017 — Voters Moved out of SANBORNTON waiting for Supervisor/Registrar Approval to Remove — Page 1

User ID : HD-SDODGE

Removal Date	Name (Previous Name)	Old Address	Old Ward	New Address	New Ward	Voter ID
11/08/2016	[redacted]	[redacted]	00	[redacted]	03	[redacted]
11/08/2016			00		00	
11/08/2016			00		05	

Print List and pull Active Voter Reg. Cards from Your **ACTIVE FILE**

If your town has been diligent about filing removed voters in the **IN-ACTIVE FILE** they will not be in your **ACTIVE FILE**

Inquiry - Voters Moved Out of City/Town — HD-SDODGE / SANBORNTON

The following voters have registered to vote in another New Hampshire City/Town. These voters are no longer on your checklist.

Review and print the list of voters. Pull the paper voter registration from your "Active" file and put them in your "Inactive" file. Retention law RSA 33-A:3-a, requires you to retain these forms for 7 years from the date of removal.

Voters Who Have Moved from your city/town:

	Removal Date	Status	Name (Previous Name)	Old Address	Old Ward	New Address	New Ward
☐	01/01/2019	Active	[redacted]		00		00
☐	11/06/2018	Active			00		00
☐	11/06/2018	Active			00		00
☐	11/06/2018	Active			00		00
☐	11/06/2018	Active	SAR		00		00
☐	11/06/2018	Active	MEA		00		08
☐	01/01/2019	Removed			00		00
☐	11/06/2018	Active			00		01

[redacted]

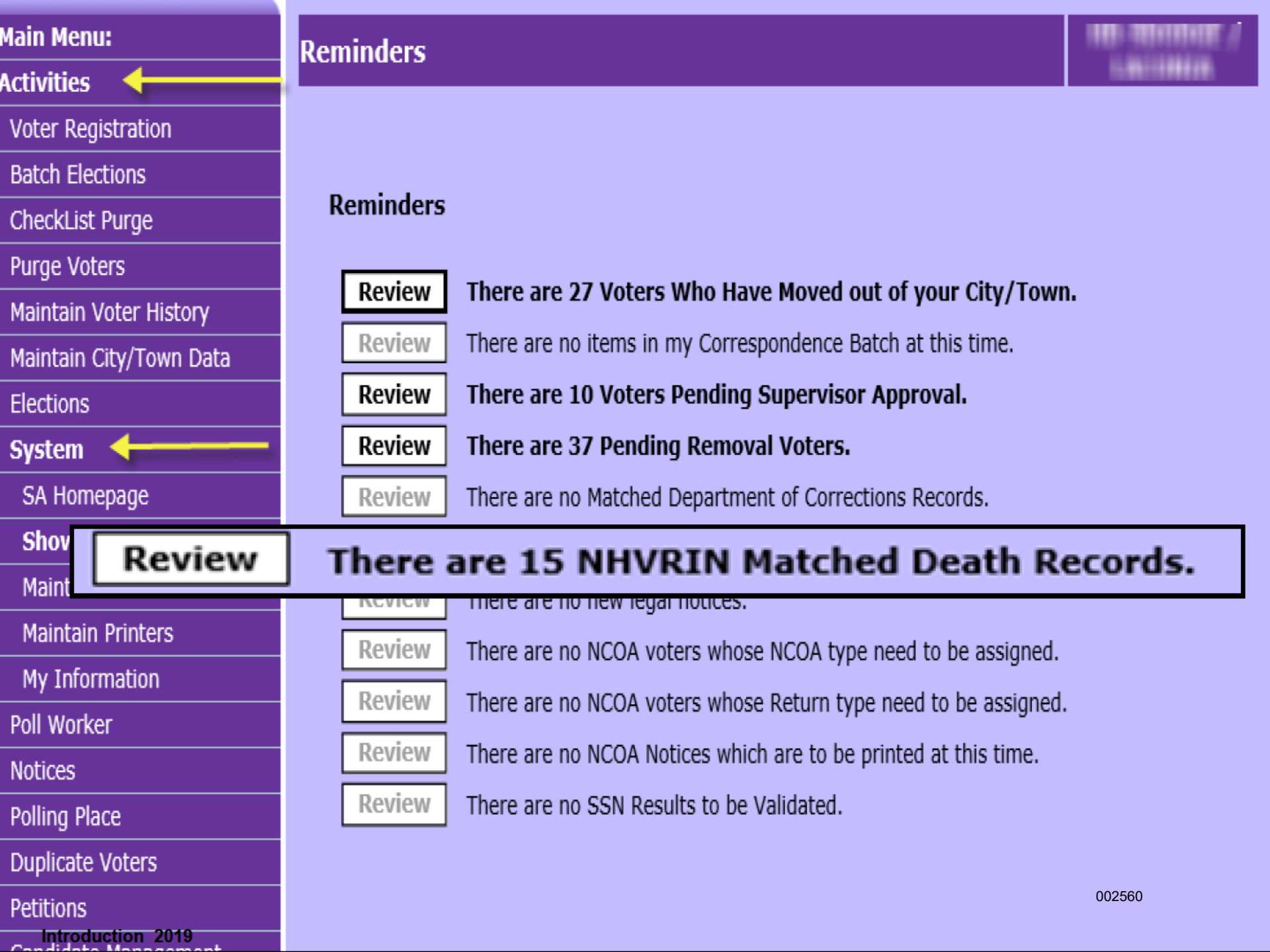
Moved to another city/town 11/08/2016 — Moved to another city/town 11/08/2016 — Moved to another city/town 11/08/2016

1 2 3

Next 90 | << Go to Page No.

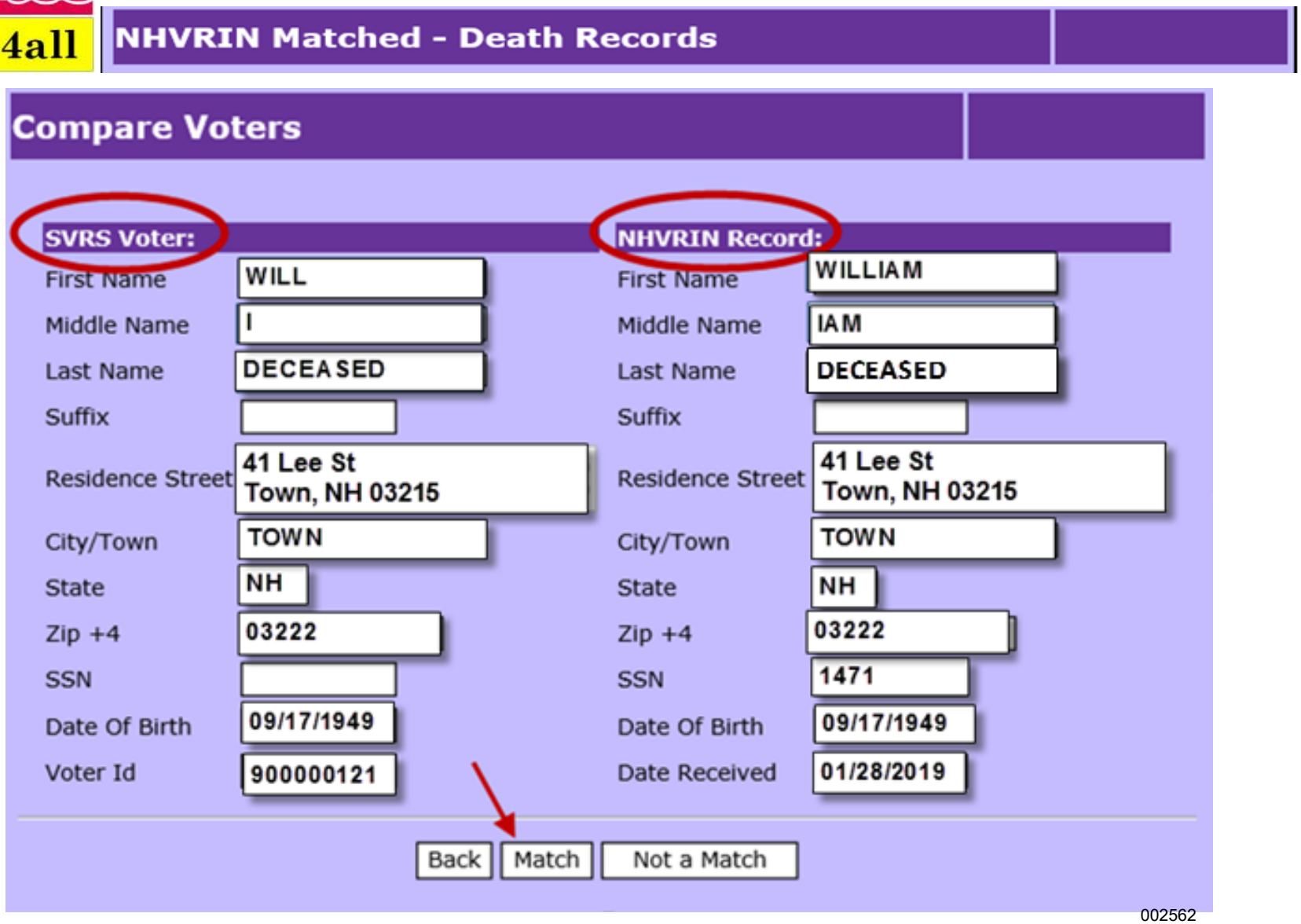
Select All | Print List | Print Labels | Approve Moved Voters

You may Print Labels with removal date and affix to pulled Reg. Card & file in **IN-ACTIVE FILES**


Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
System
SA Homepage
Maintain Printers
My Information
Poll Worker
Notices
Polling Place
Duplicate Voters
Petitions
Reminders
Reminders
Review
There are 27 Voters Who Have Moved out of your City/Town.
Review
There are no items in my Correspondence Batch at this time.
Review
There are 10 Voters Pending Supervisor Approval.
Review
There are 37 Pending Removal Voters.
Review
There are no Matched Department of Corrections Records.
Review
There are 15 NHVRIN Matched Death Records.
Review
There are no NCOA voters whose NCOA type need to be assigned.
Review
There are no NCOA voters whose Return type need to be assigned.
Review
There are no NCOA Notices which are to be printed at this time.
Review
There are no SSN Results to be Validated.
002560
Introduction 2019

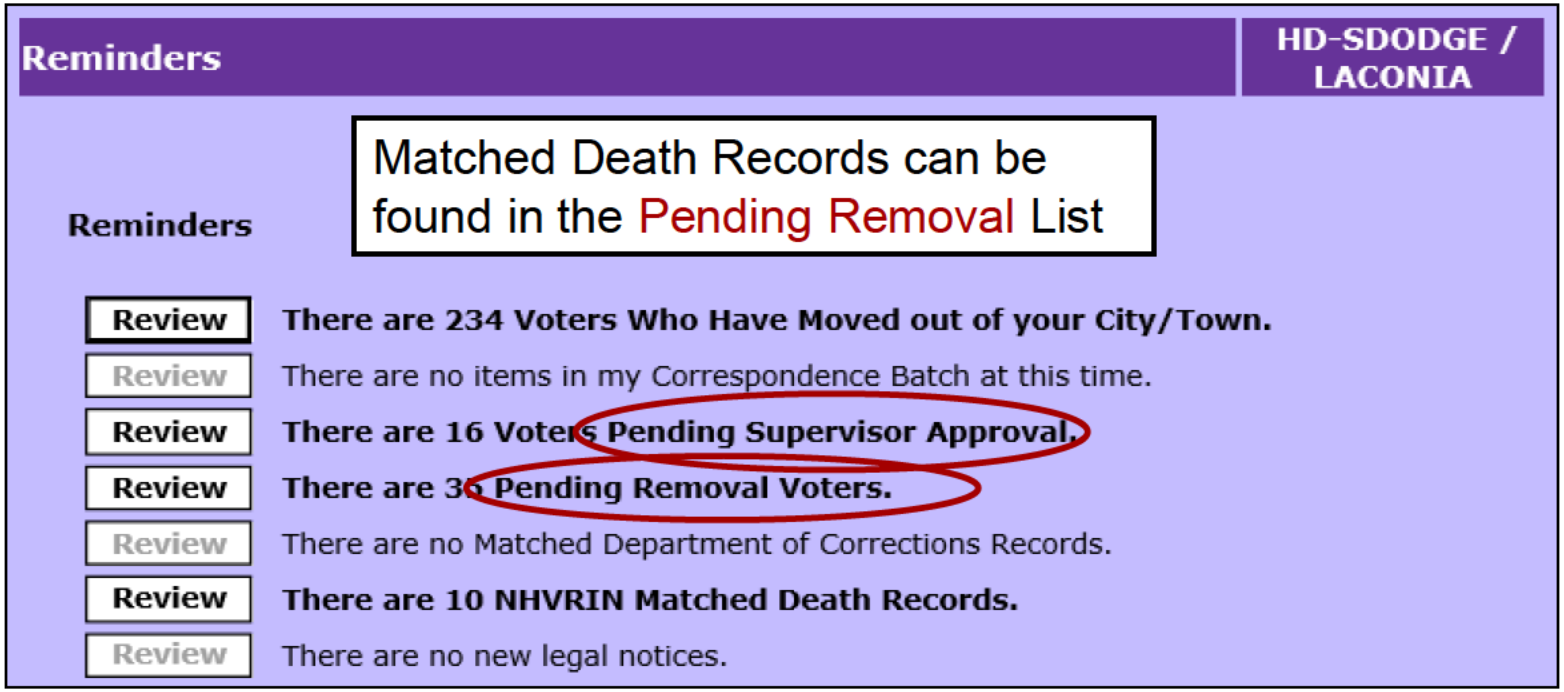
Matched Death Record– Show Reminder Screen

Matched Death Record– Show Reminder Screen



Introduction to ElectioNet

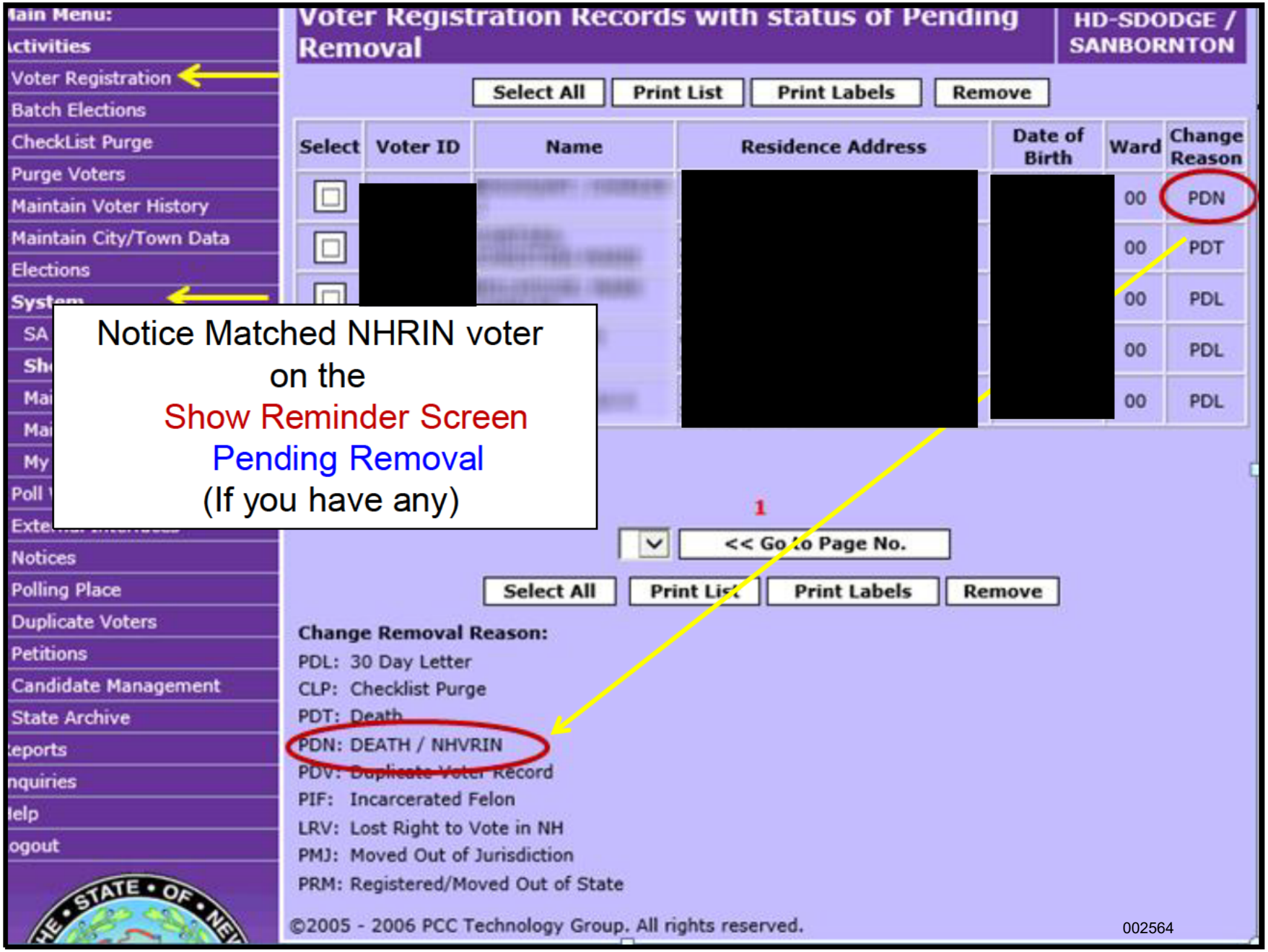
Show Reminder Screen



- **Click on Your Review button for Pending Removals if it is black**
- **Take a look at Your Pending Removals if you have any.**

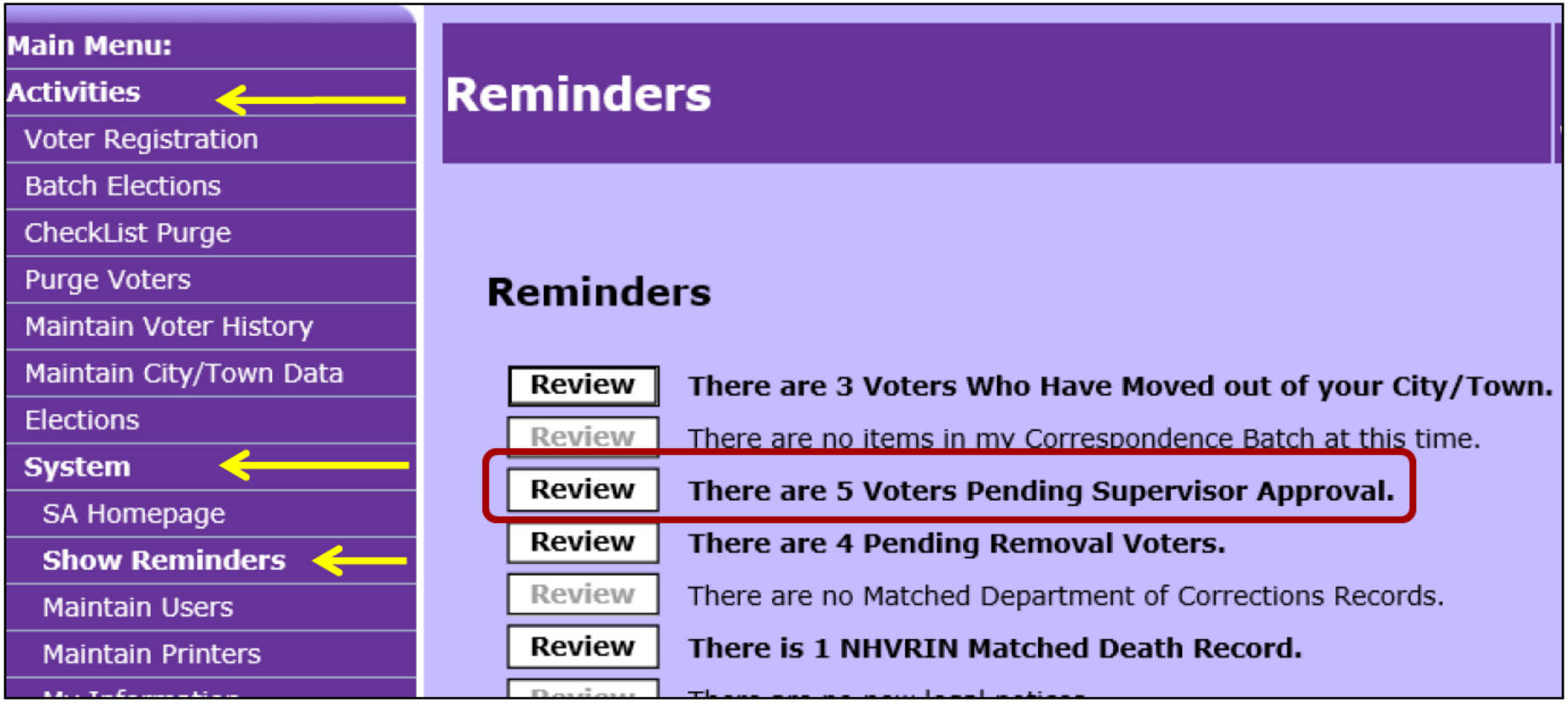
002563

Matched Death Record– Show Reminder Screen

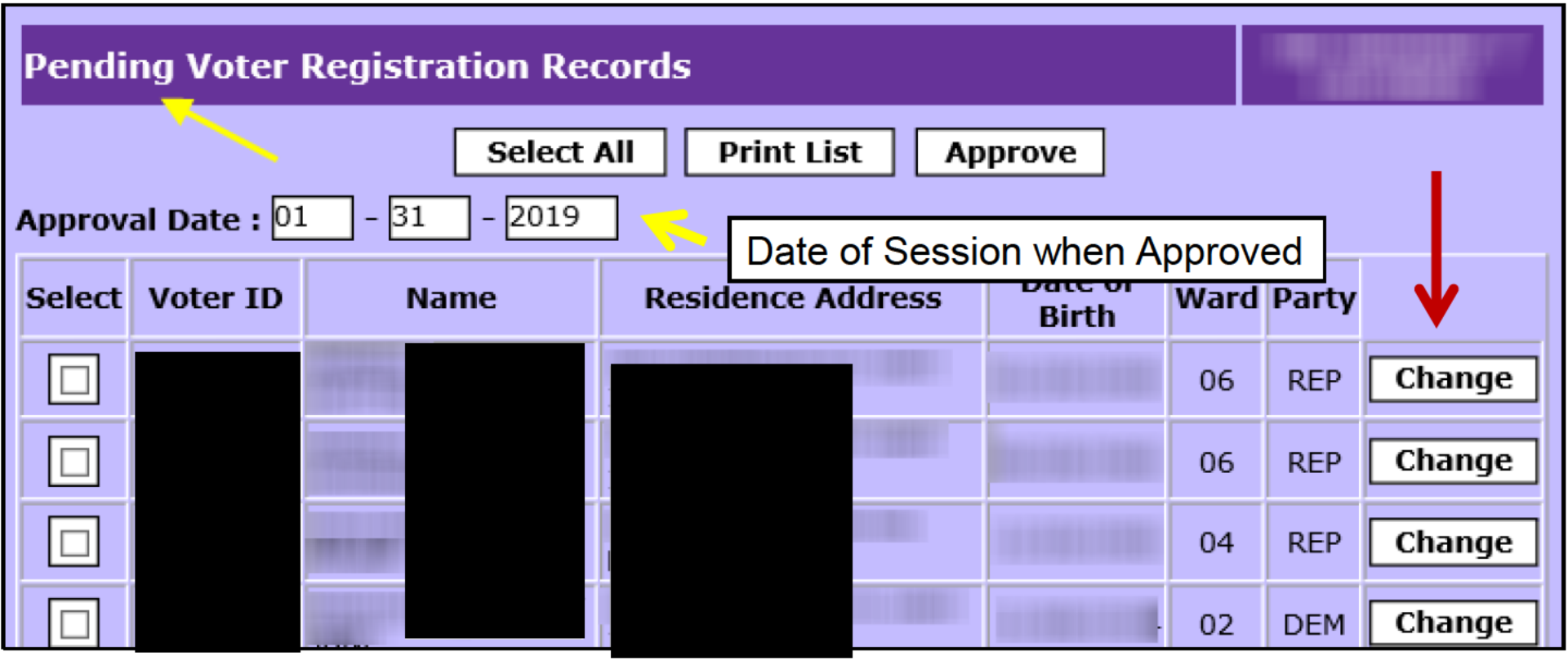


Introduction to ElectioNet

- **SHOW REMINDER SCREEN – Pending Approval**



- **SHOW REMINDER SCREEN – Pending Approval**



- Remember -

Always Print Lists from Reminder Screen before Approving


Demo
Pending
Approval

Introduction to ElectioNet

ElectioNet Help:

Navigate to Help

Click Instructions

Do some browsing and see what you can find

002568

Introduction to ElectioNet

Help / Instructions

Find a wide array of instructions and forms.

* Absentee Ballots
* Affidavits
* Ballot Clerk Procedure
* Label Instructions
*Summary & Work Sheets for end of Election reporting
*Election Procedures Primary/General
*IT Issue Instructions
*Learn How to make Labels
* UOCAVA
*Voter Registration Forms

And Many More Topics

How Do I Do That?

Help/Instructions

Introduction to ElectioNet

- Main Menu:
- Activities
  - Voter Registration
  - Batch Elections
  - 30 Day Letter
  - Maintain Voter History
  - **Maintain City/Town Data**
    - City/Town Data
    - Maintain Clerk
    - Add Street
    - Maintain Street
    - Street Name Change

SANBORNTON

Maintain Clerk

City/Town Name: SANBORNTON
City/Town Code: 20901

Select for letterhead

City/Town Clerk

First Name	[redacted]	Title	TOWN CLERK
Middle Name		Term Exp. Date (mm/dd/yyyy)	03 / 12 / 2019
Last Name	[redacted]		
Suffix			

Address

Street Number	[redacted]		
Street Name/PO Box	[redacted]		
Unit			
City/Town	SANBORNTON		
State	New Hampshire	Election Day #	Cell Phone
Zip	03269 -	Day After Election #	Office Phone
		Email - Public	[redacted]
		Email - Private	

Mailing Address (if different from the City/Town Address)

Street Number	
Street Name/PO Box	[redacted]
Unit	
City/Town	SANBORNTON
State	New Hampshire
Zip	03269 -

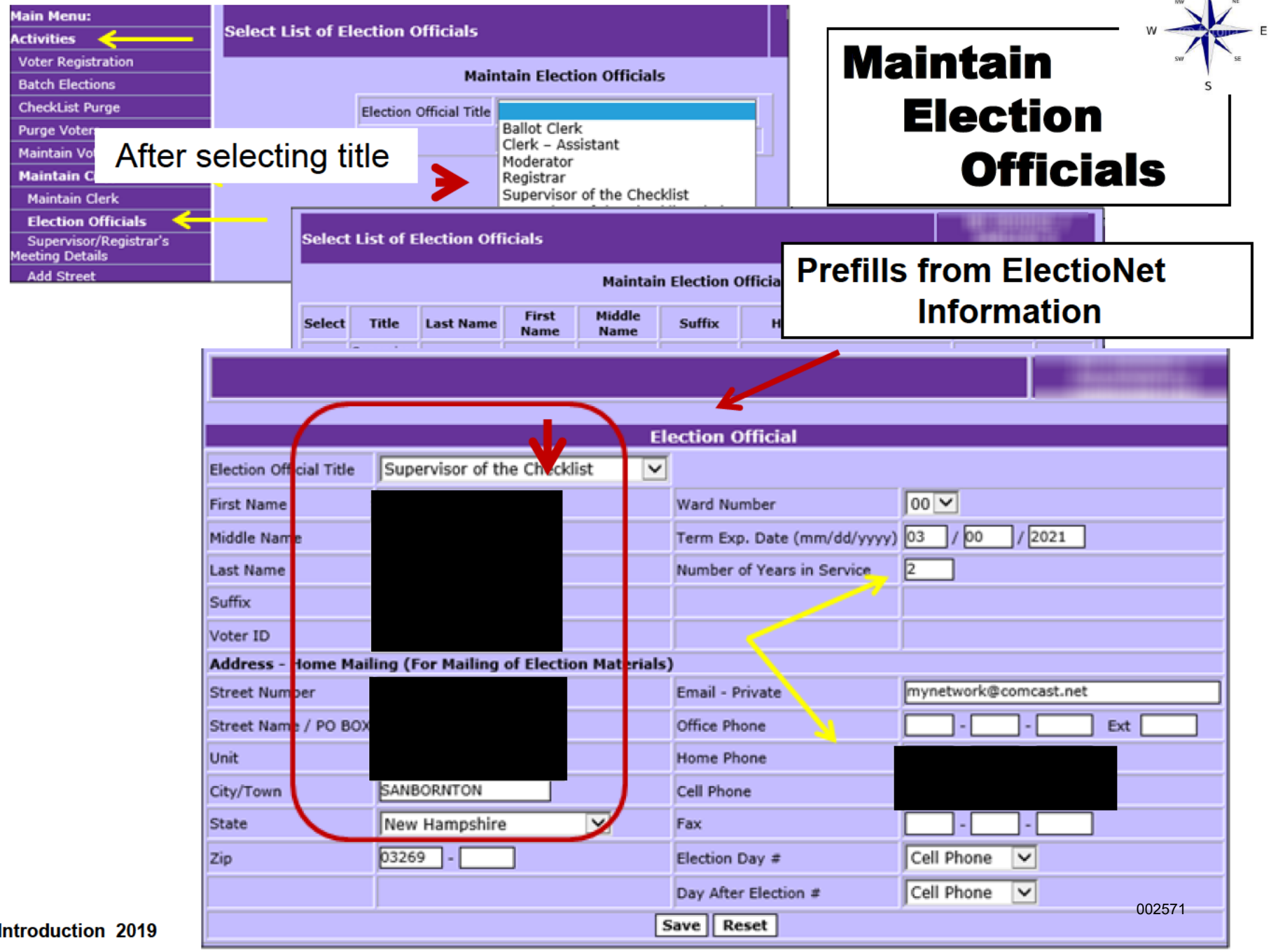
City/Town Deputy Clerk

First Name	[redacted]	Title	DEPUTY
Middle Name		Term Exp. Date (mm/dd/yyyy)	03 / 12 / 2019
Last Name	[redacted]	Number of Years in Service	1
Suffix			

Address (if different from the City/Town Address) **Same as the City/Town Clerk** ☐

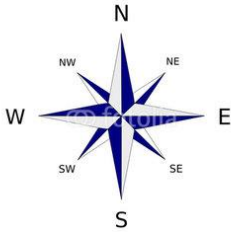
Street Number	[redacted]	Office Phone	603 - 286 - 4034 Ext
Street Name/PO Box		Home Phone	[redacted]
Unit		Cell Phone	
City/Town	SANBORNTON	Election Day #	Cell Phone

Maintain Clerks Should be kept Current



Maintain Election Officials

Chapter Review



What procedure has to happen to Remove or Approve a Voter?

There must be a Public Session with a quorum of SOC in attendance

Do you need to publicize a Session?

Yes

Where would you post publications of meetings?

2 postings-city/town Website **or** Newspaper and with the Posted Checklist

Where do you find your voters that need Approval?

Activities>System>Show Reminders

When working in the Show Reminders what is the 1st thing you should do?

Print your List

Do you need to keep Meeting Minutes?

Yes it is a must

Introduction to ElectioNet

Inquiries

Lets Look Up

Introduction to ElectioNet

Inquiries – Voter Registration:

- Allows users to locate records efficiently
- Allows users to perform a variety of broad or narrow searches
    - Full name searches are not required
    - **DOB is not allowed**
    - User can search for voter records on a specific street in a specific NH town
- Broad searches in Inquiries helps prevent **Duplicate Voter records**
- Copy voter ID# onto clipboard to use on another screen

Introduction to ElectioNet

Inquiries – Voter Registration:

- ***Less*** information = ***More*** records to review
- ***More*** information = ***Less*** records to review
- Inquiries allows users to ***view*** voter information
- See hand out: Search – Inquiries & Activities


Instructor
Demo
Inquiries

Introduction to ElectioNet

Print a Voter Registration or Wallet Card

Go to Inquiries>Voter Registration

1. Default **Search Type to City/Town** (@ top of page)
2. Under Voter Name **type in YOUR last and first name**
   Click Search **at bottom of page**
3. Click **Scan/Print button**
4. Click **Reprint Voter Registration Card**
5. Notice the Reg. Card has **two Scroll Bars** on the right

If you can't see a print box scroll down using the outer bar

The inner bar allows you to scroll the registration form

Do not click the Print Button

002577

Introduction to ElectioNet

Find the following voters in:
Inquiries / Voter Registration

002578

PLEASE PRINT OR TYPE

NEW HAMPSHIRE VOTER REGISTRATION FORM

RSA 654:7

1. LAST NAME (including suffix if any)	FIRST NAME	FULL MIDDLE NAME
Brassard	Sallie	Raye

2. DOMICILE ADDRESS (Street & House (Apt.) Number)	TOWN OR CITY	City Ward	ZIP CODE
#7 Any Town	Your Town		Your Zip

3. MAILING ADDRESS (If different from domicile address)	TOWN OR CITY	STATE	ZIP CODE

4. PLACE OF BIRTH (Town/City and State)	COUNTRY (If not USA)	DATE OF BIRTH
Westerlev Rhode Island		01-17-1946

5. a. ARE YOU A CITIZEN OF THE UNITED STATES? YES X NO _____
b. IF NATURALIZED CITIZEN, GIVE NAME OF COURT WHERE NATURALIZED (Town/City and State)

DATE NATURALIZED

6. PLACE LAST REGISTERED TO VOTE (Street & House (Apt.) Number) (Town or City & Ward) (State and Zip Code)

1014B South Lomaza Dr San Francisco Ca 74741

7. NAME UNDER WHICH PREVIOUSLY REGISTERED, IF DIFFERENT	8. PARTY AFFILIATION (if any)

9. DRIVER'S LICENSE NUMBER	STATE (If not NH)	IF NO VALID DRIVER'S LICENSE, PROVIDE THE LAST FOUR DIGITS OF YOUR SOCIAL SECURITY NUMBER
L12154218	CA	5 8 8 7

___NEW REGISTRATION – I am NOT registered to vote in NH

X TRANSFER – I am registered to vote in NH and have moved my voting domicile to a new town or ward in NH.

___NAME CHANGE or ADDRESS UPDATE – I am registered to vote in this town/ward and have changed my name or address.

Bank Loan

AFFIDAVIT

My name is Sallie Brassard. I am today registering to vote in the city/town of Your City/Town, New Hampshire. If a city, ward number _____.

I understand that to vote in this ward/town, I must be 18 years of age, I must be a United States citizen, and I must be domiciled in this ward/town.

I understand that a person can claim only one state and one city/town as his or her domicile at a time. A domicile is that place, to which upon temporary absence, a person has the intention of returning. By registering or voting today, I am acknowledging that I am not domiciled or voting in any other state or any other city/town.

In declaring New Hampshire as my domicile, I realize that I am not qualified to vote in the state or federal elections in another state.

If I have any questions as to whether I am entitled to vote in this city/town, I am aware that a supervisor of the checklist is available to address my questions or concerns.

I acknowledge **that I have read and understand the above qualifications** for voting and do hereby swear, under the penalties for voting fraud set forth below, that I am qualified to vote in the above-stated city/town, and, if registering on election day, that I have not voted and will not vote at any other polling place this election.

Sallie Brassard
Signature of Applicant

Date 0-0-19

Received by Marie Tilton

Approved by Tom Wilder
SUPERVISOR OF CHECKLIST/REGISTRAR OF VOTERS

In accordance with RSA 659:34, the penalty for knowingly or purposefully providing false information when registering to vote or voting is a class A misdemeanor with a maximum sentence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently registering to vote or voting is subject to a civil penalty not to exceed $5,000.

July 2016

002579

Chapter Review

Why is it so important to do an Inquiries Search before entering in a Voter?

Each voter in ElectioNet should be associated with only **One Voter ID#**

Should you use a DOB when doing a search in Inquiries?

No you will get a Pop up "No Voter Found"

If a voter record matches but the DOB is different should the voter be taken?

No, contact the town/city, have them check the registration form-take only if it matches. Never change a DOB unless you have positive verification

Why would you do a search using a partial name?

You get a wider search which may find a voter with a misspelled name or even a name change

PLEASE PRINT OR TYPE

NEW HAMPSHIRE VOTER REGISTRATION FORM RSA 654:7

1. LAST NAME (including suffix if any) | FIRST NAME | FULL MIDDLE NAME

2. DOMICILE ADDRESS (Street & House (Apt.) Number) | TOWN OR CITY | City Ward | ZIP CODE

3. MAILING ADDRESS (If different from domicile address) | TOWN OR CITY | STATE | ZIP CODE

4. PLACE OF BIRTH (Town/City and State) | COUNTRY (If not USA) | DATE OF BIRTH

5. a. ARE YOU A CITIZEN OF THE UNITED STATES? YES _____ NO _____ | DATE NATURALIZED
b. IF NATURALIZED CITIZEN, GIVE NAME OF COURT WHERE NATURALIZED (Town/City and State)

6. PLACE LAST REGISTERED TO VOTE (Street & House (Apt.) Number) | (Town or City & Ward) | (State and Zip Code)

7. NAME UNDER WHICH PREVIOUSLY REGISTERED, IF DIFFERENT | 8. PARTY AFFILIATION (if any)

9. DRIVER'S LICENSE NUMBER | STATE (If not NH) | IF NO VALID DRIVER'S LICENSE, PROVIDE THE LAST FOUR DIGITS OF YOUR SOCIAL SECURITY NUMBER

___ **NEW REGISTRATION** – I am NOT registered to vote in NH

___ **TRANSFER** – I am registered to vote in NH and have moved my voting domicile to a new town or ward in NH.

___ **NAME CHANGE or ADDRESS UPDATE** – I am registered to vote in this town/ward and have changed my name or address.

AFFIDAVIT

My name is _____. I am today registering to vote in the city/town of _____, New Hampshire. If a city, ward number _____.

I understand that to vote in this ward/town, I must be 18 years of age, I must be a United States citizen, and I must be domiciled in this ward/town.

I understand that a person can claim only one state and one city/town as his or her domicile at a time. A domicile is that place, to which upon temporary absence, a person has the intention of returning. By registering or voting today, I am acknowledging that I am not domiciled or voting in any other state or any other city/town.

In declaring New Hampshire as my domicile, I realize that I am not qualified to vote in the state or federal elections in another state.

If I have any questions as to whether I am entitled to vote in this city/town, I am aware that a supervisor of the checklist is available to address my questions or concerns.

I acknowledge **that I have read and understand the above qualifications** for voting and do hereby swear, under the penalties for voting fraud set forth below, that I am qualified to vote in the above-stated city/town, and, if registering on election day, that I have not voted and will not vote at any other polling place this election.

_____ Date _____
Signature of Applicant

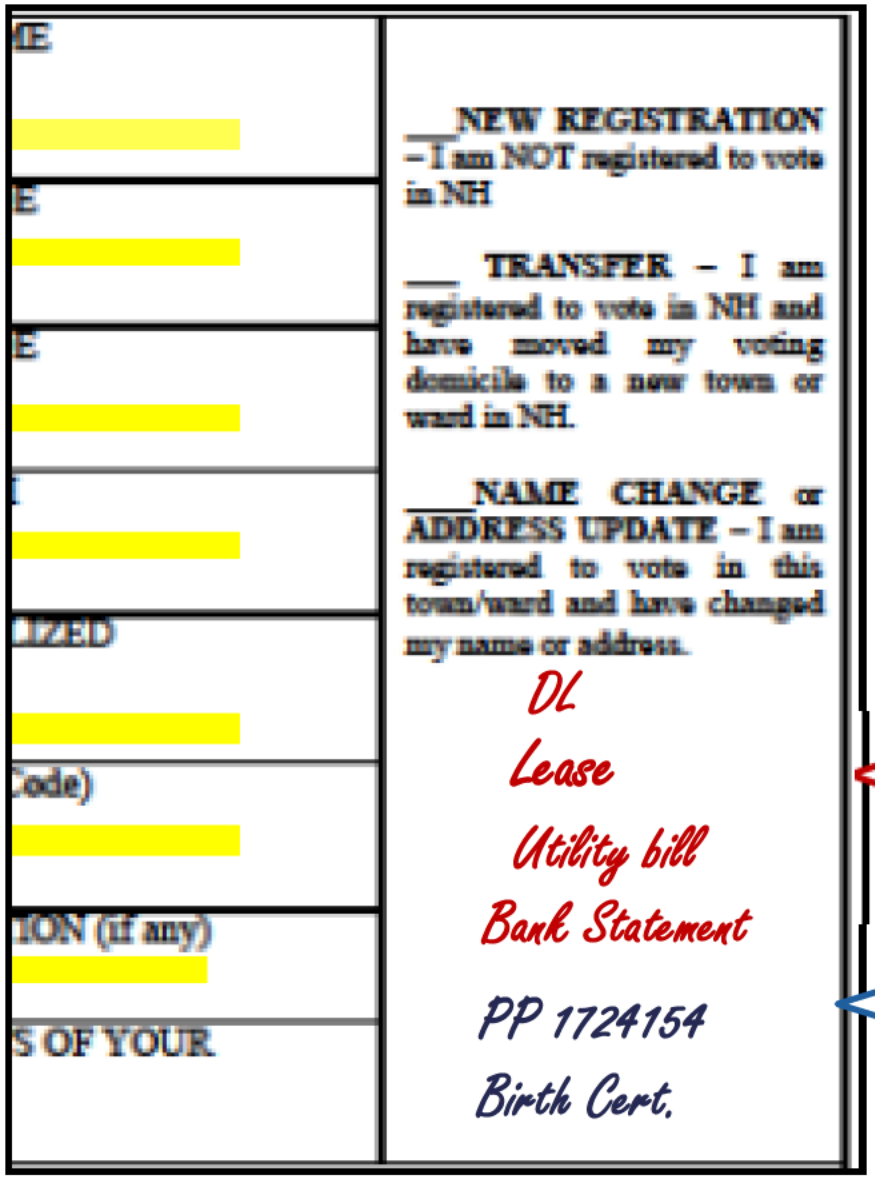
Received by _____

Approved by _____
SUPERVISOR OF CHECKLIST/REGISTRAR OF VOTERS

In accordance with RSA 659:34, the penalty for knowingly or purposefully providing false information when registering to vote or voting is a class A misdemeanor with a maximum sentence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently registering to vote or voting is subject to a civil penalty not to exceed $5,000.

July 2016

002581



With out the proper information you will not be able to enter the voter into your town/city.

You will need to notify the voter that the registration form was not complete and they will need to supply the missing information.

Best Practice:
Read Line by Line

Record what was shown for **Domicile**

If proof was shown for **Age,Citizenship** and or **Indentity,**

Refer to EPM

Pg. 19-21

002582

Voter Registration

If the applicant does not have the necessary documentation to register to vote:

- ✓ There are two types of Affidavits available which will help the voter complete the Voter Registration Form.
- ✓ Is the voter missing proof of **Domicile?**
- ✓ Is the voter missing proof of **Citizenship, Age** or **Identity?**

Voter Registration Affidavits

Domicile Affidavit

Qualified Voter Affidavit

Help/Instructions

DOMICILE AFFIDAVIT
(RSA 654:12)

Please print. Date: _____

Full Name: _____

Current Domicile Address: _____
(Street and House (Apt) Number) (Town or City/State/Zip Code) (Ward)

_____
(Town or City/State/Zip Code)

_____

_____

_____
Year

Date of birth: _____

Address of last previous domicile: _____
(Street and House (Apt) Nu

_____
(Town or City) (State)

I hereby swear and affirm, under the penalties for voting fraud set forth
necessary documents to prove my domicile and that my established domicile
above. I understand that a person can claim only one state and one city/tow
that place, to which upon temporary absence, a person has the intention of
acknowledging that I am not domiciled or voting in any other city/town, an
information above is true and correct.

_____
(Signature of applicant)

In accordance with RSA 659:34, the penalty for knowingly or purposefully providing false information when registering to vote or voting is a class A misdemeanor with a maximum sentence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently registering to vote or voting is subject to a civil penalty not to exceed $5,000.

On the date shown above, before me, _____ appeared _____
(print name of person sworn before as indicated below) (print name of person whose signature is being notarized/witnessed)

[known to me or satisfactorily proven (circle one)] to be the person whose name appears above, and he or she subscribed his or her name to the foregoing affidavit and swore that the facts contained in this affidavit are true to the best of his or her knowledge and belief.

_____
(moderator, deputy moderator, assistant moderator, town clerk, deputy town clerk, city clerk, deputy city clerk, ward clerk, selectman, supervisor of the checklist, registrar, deputy registrar, notary public, or justice of the peace)

03/2017

QUALIFIED VOTER AFFIDAVIT
(Identity, Citizenship, Age)
(RSA 654:12)

Please Print. Date: _____

Full Name: _____

Name at birth if different: _____

Place of birth: _____

Date of birth: _____

Place of Naturalization: _____

Date of Naturalization: _____

Domicile Address: _____
(Street & House (Apt. Numbe

Mailing Address (if different) _____

Telephone number (*requested but optional*) _____

but optional) _____

d set forth below, that I am not in possession of some or all of the that I am the identical person whom I represent myself to be, that I States citizen, that I am at least 18 years of age as of this date or wledge and belief the information above is true and correct.

_____

or purposefully providing false information when registering to vote or vo ence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently reg subject to a civil penalty not to exceed $5,000.

On the date shown above, before me, _____ appeared _____
(print name of person sworn before as indicated below) (print name of person whose signature is being notarized/witnessed)

[known to me or satisfactorily proven (circle one)] to be the person whose name appears above, and he or she subscribed his or her name to the foregoing affidavit and swore that the facts contained in this affidavit are true to the best of his or her knowledge and belief.

This affidavit was executed for purposes of proving (check all that apply):

[ ] Identity [ ] Citizenship [ ] Age

_____
(moderator, deputy moderator, assistant moderator, town clerk, deputy town clerk, city clerk, deputy city clerk, ward clerk, selectman, supervisor of the checklist, registrar, deputy registrar, notary public, or justice of the peace)

Introduction to ElectioNet

WORK ZONE

Activities - Voter Registration:

"Activities" is where you "WORK"

Activities->Voter Registration->Add/Change Voter

- Searches for an exact match to a voter record can be selected if moving to your town or changing an address within your town.
- The search criteria and results are not the same as the Inquiries search function.
- No user should be in "Activities", *without first searching for the voter in* ***"Inquiries"*** *first.*

002585

PLEASE PRINT OR TYPE

NEW HAMPSHIRE VOTER REGISTRATION FORM RSA 654:7

1. LAST NAME (including suffix if any): Pick a Color for Last Name
FIRST NAME: Any First Name
FULL MIDDLE NAME: Any Middle Name

2. DOMICILE ADDRESS (Street & House (Apt.) Number): Your Home Address
TOWN OR CITY: Your Town
City Ward:
ZIP CODE: Your Zip

3. MAILING ADDRESS (If different from domicile address): PO Box 123
TOWN OR CITY: Your Town
STATE:
ZIP CODE: Your Zip

4. PLACE OF BIRTH (Town/City and State): Any city/town Any State
COUNTRY (If not USA): USA
DATE OF BIRTH: 01-01-1981

5. a. ARE YOU A CITIZEN OF THE UNITED STATES? YES X NO ?
b. IF NATURALIZED CITIZEN, GIVE NAME OF COURT WHERE NATURALIZED (Town/City and State)
DATE NATURALIZED

6. PLACE LAST REGISTERED TO VOTE (Street & House (Apt.) Number): 1252 Storrow Drive Apt 342D
(Town or City & Ward): Boston Ma
(State and Zip Code): 02010

7. NAME UNDER WHICH PREVIOUSLY REGISTERED, IF DIFFERENT

8. PARTY AFFILIATION (if any): Rep Dem Und

9. DRIVER'S LICENSE NUMBER: NHL 29848909
STATE (If not NH):
IF NO VALID DRIVER'S LICENSE, PROVIDE THE LAST FOUR DIGITS OF YOUR SOCIAL SECURITY NUMBER: 1 2 3 4

X
___ NEW REGISTRATION – I am NOT registered to vote in NH

___ TRANSFER – I am registered to vote in NH and have moved my voting domicile to a new town or ward in NH.

___ NAME CHANGE or ADDRESS UPDATE – I am registered to vote in this town/ward and have changed my name or address.

Enter what you saw for domicile such as:
DL or
Utility Bill
Lease
Bank Statement
Etc.

AFFIDAVIT

My name is _____. I am today registering to vote in the city/town of _____, New Hampshire. If a city, ward number _____.

I understand that to vote in this ward/town, I must be 18 years of age, I must be a United States citizen, and I must be domiciled in this ward/town.

I understand that a person can claim only one state and one city/town as his or her domicile at a time. A domicile is that place, to which upon temporary absence, a person has the intention of returning. By registering or voting today, I am acknowledging that I am not domiciled or voting in any other state or any other city/town.

In declaring New Hampshire as my domicile, I realize that I am not qualified to vote in the state or federal elections in another state.

If I have any questions as to whether I am entitled to vote in this city/town, I am aware that a supervisor of the checklist is available to address my questions or concerns.

I acknowledge **that I have read and understand the above qualifications** for voting and do hereby swear, under the penalties for voting fraud set forth below, that I am qualified to vote in the above-stated city/town, and, if registering on election day, that I have not voted and will not vote at any other polling place this election.

_____ Date _____
Signature of Applicant

Received by _____

Approved by _____
SUPERVISOR OF CHECKLIST/REGISTRAR OF VOTERS

In accordance with RSA 659:34, the penalty for knowingly or purposefully providing false information when registering to vote or voting is a class A misdemeanor with a maximum sentence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently registering to vote or voting is subject to a civil penalty not to exceed $5,000.

July 2016

002586

Introduction to ElectioNet

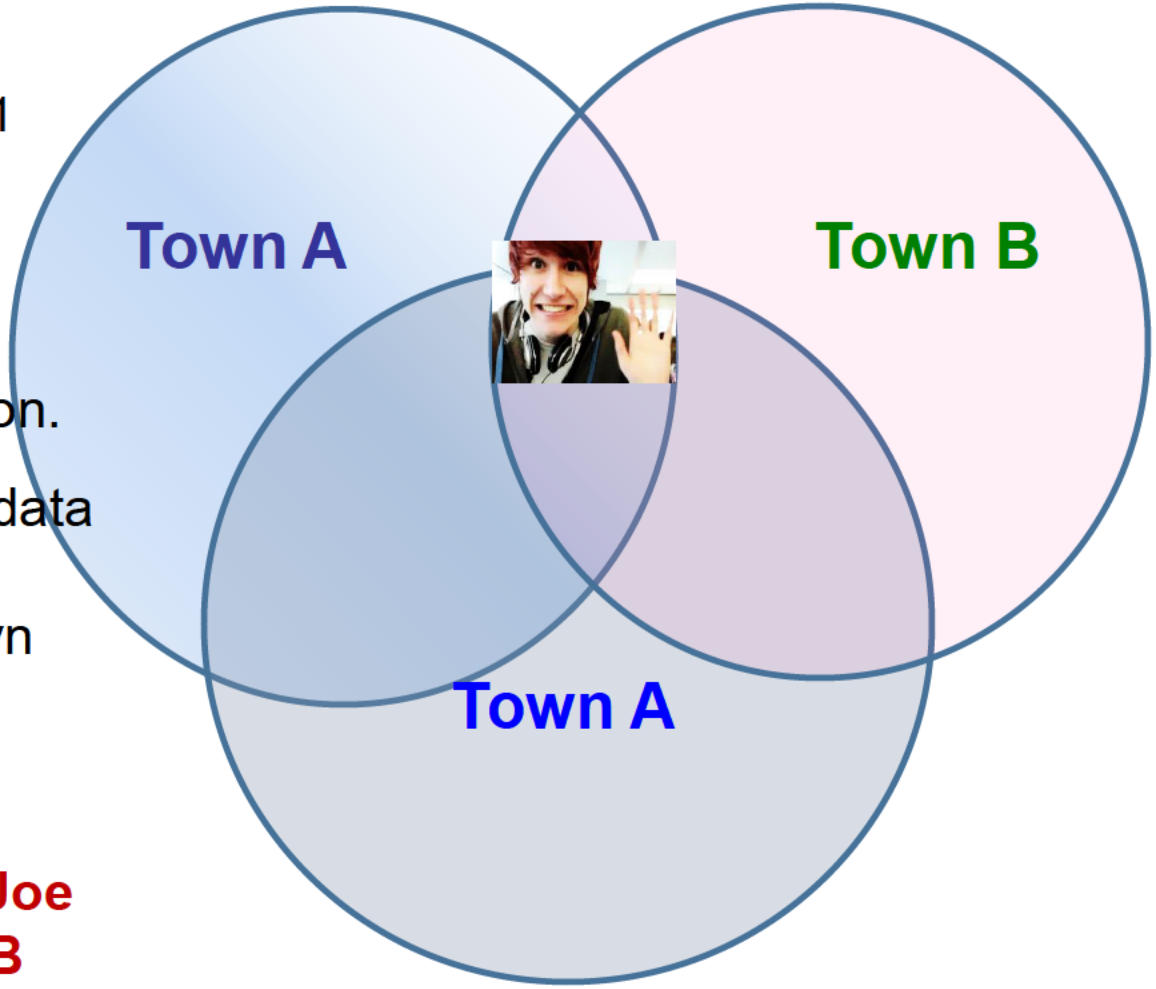
WORK ZONE

“People are on the Move”

Introduction to Electio*Net*

WORK ZONE

- Joe Voter moved to Town **A**, registered to vote April 1
- Joe Voter then moved to Town **B** and registered to vote. **B** meets regularly & approved @ their next session.
- Town **A** delayed entering data in Electio*Net* and thus Pulled Joe Voter from Town **B** and approved him in Town **A**. Town **B** had a special election and Joe was not on the checklist. **Joe had to register in town B - again -**



002588

Introduction to ElectioNet

WORK ZONE

Before entering a New Voter to your city/town what is your first step?

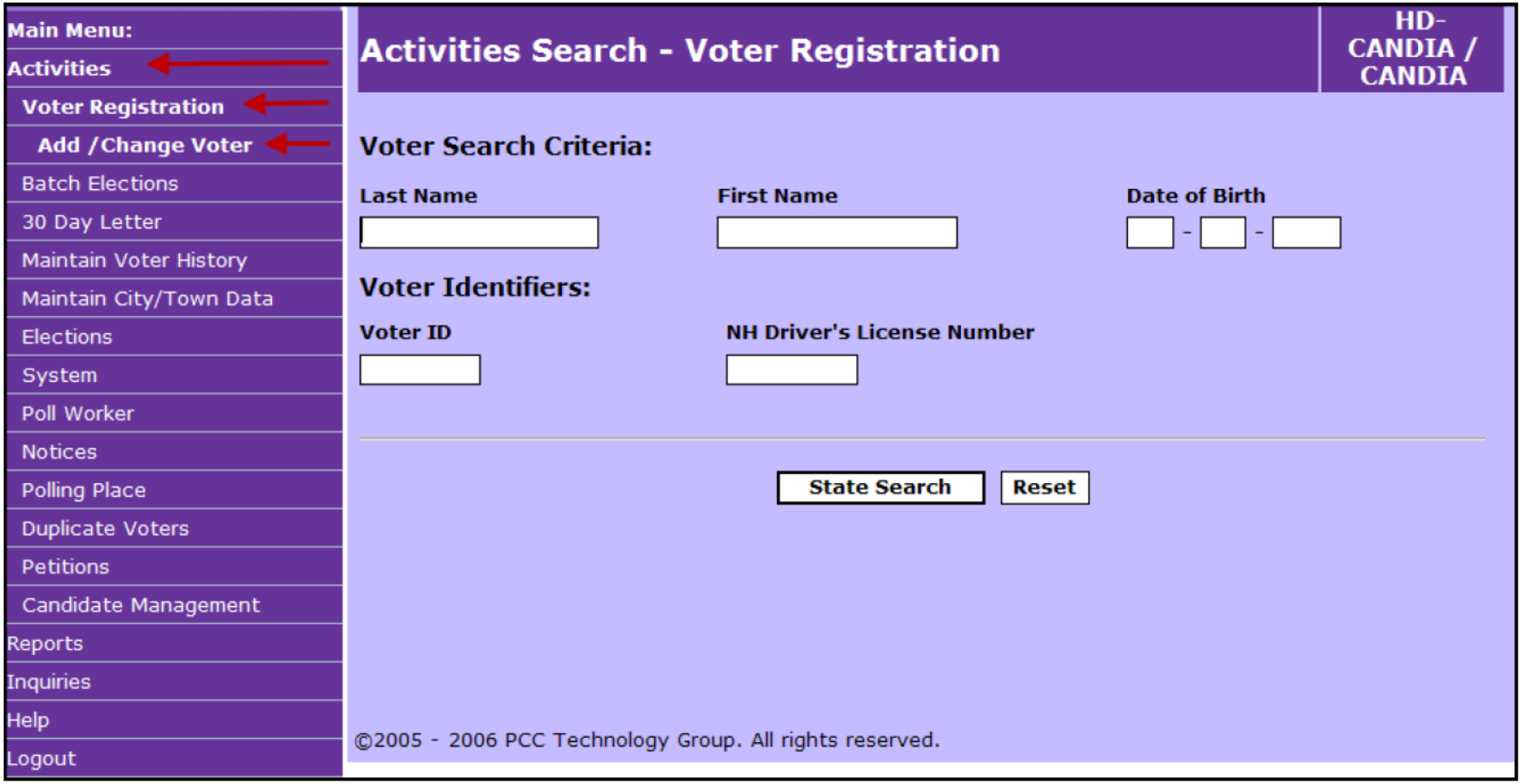
INQUIRIES>VOTER REGISTRATION

002589

Introduction to ElectioNet

WORK ZONE

Main Menu/Activities>Voter Registration>Add Change

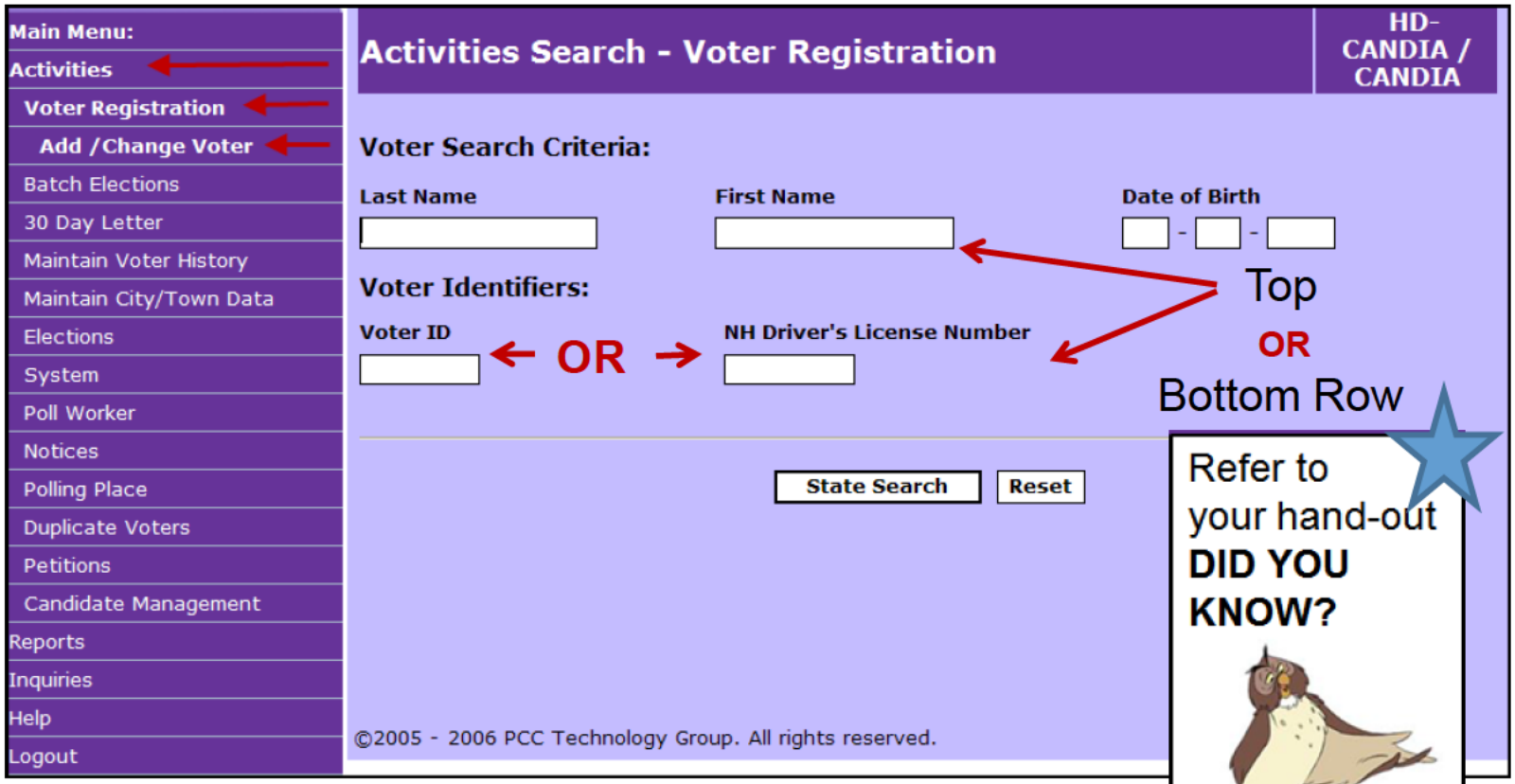


002590

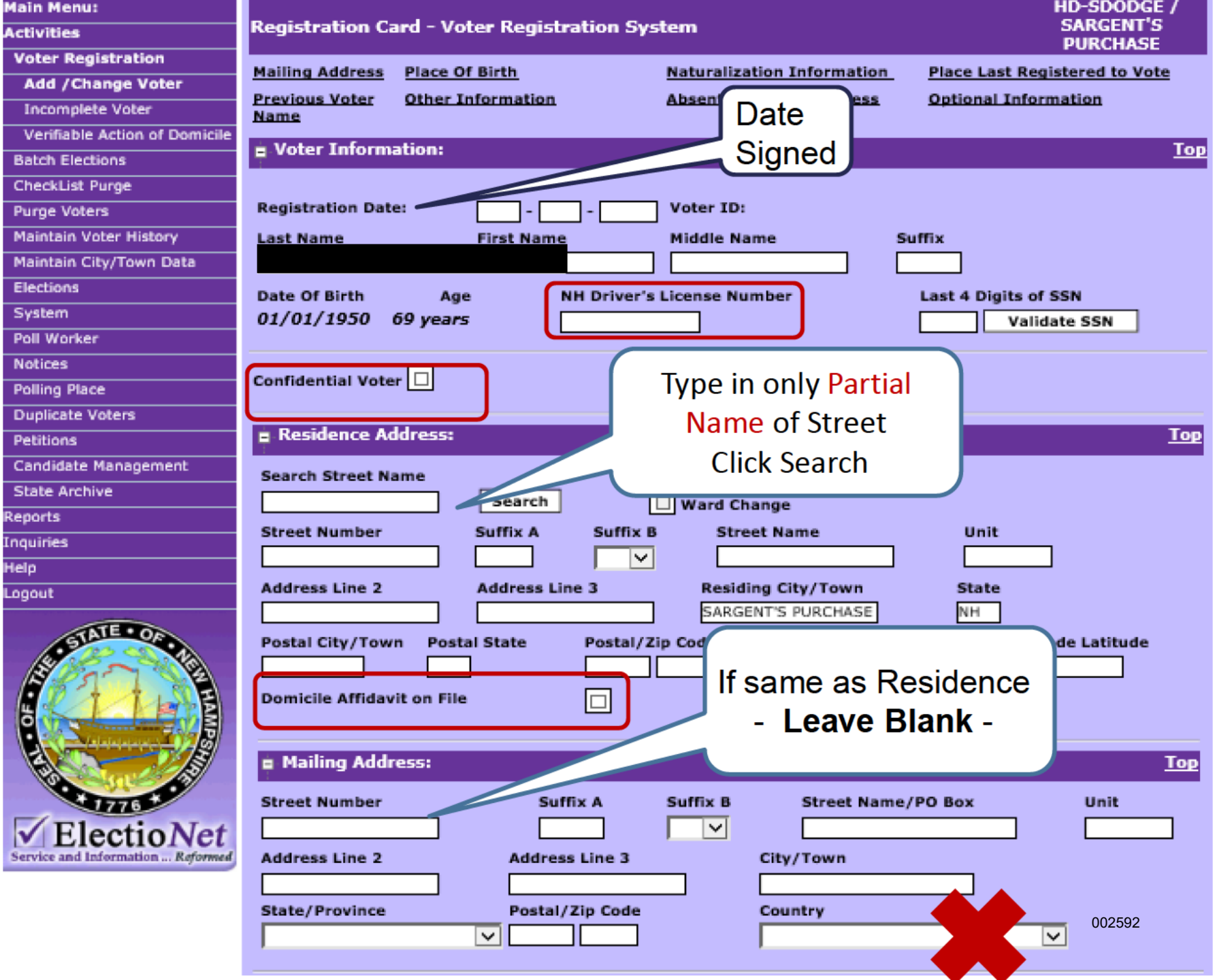
Introduction to ElectioNet

WORK ZONE

Activities - Voter Registration Search:



002591


Main Menu:
Activities
Voter Registration
Add /Change Voter
Incomplete Voter
Verifiable Action of Domicile
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
System
Poll Worker
Notices
Polling Place
Duplicate Voters
Petitions
Candidate Management
State Archive
Reports
Inquiries
Help
Logout
ElectioNet
Service and Information ... Reformed
Registration Card - Voter Registration System
HD-SDODGE / SARGENT'S PURCHASE
Mailing Address
Place Of Birth
Naturalization Information
Place Last Registered to Vote
Previous Voter Name
Other Information
Optional Information
Date Signed
Voter Information:
Top
Registration Date:
Voter ID:
Last Name
First Name
Middle Name
Suffix
Date Of Birth
Age
01/01/1950
69 years
NH Driver's License Number
Last 4 Digits of SSN
Validate SSN
Confidential Voter
Type in only Partial Name of Street Click Search
Residence Address:
Top
Search Street Name
Search
Ward Change
Street Number
Suffix A
Suffix B
Street Name
Unit
Address Line 2
Address Line 3
Residing City/Town
SARGENT'S PURCHASE
State
NH
Postal City/Town
Postal State
Postal/Zip Cod
de Latitude
Domicile Affidavit on File
If same as Residence - Leave Blank -
Mailing Address:
Top
Street Number
Suffix A
Suffix B
Street Name/PO Box
Unit
Address Line 2
Address Line 3
City/Town
State/Province
Postal/Zip Code
Country
002592

Place Of Birth:

Top

City/Town

State/Province

Country: United States

Born Abroad to US/Naturalized Citizen ☐

Naturalized Citizen ○ Yes ◉ No

Citizen of the United States ○ Yes ○ No

Naturalization Information:

Top

Name of Court where Naturalized

City/Town

State

Date Naturalized - -

Qualified Voter Affidavit - Citizenship on file ☐

Place Last Registered to Vote

Top

Street Number | Suff A | Suff B | Street Name/PO Box | Unit

Address line 2 | Address line 3 | City Ward/Town | Ward

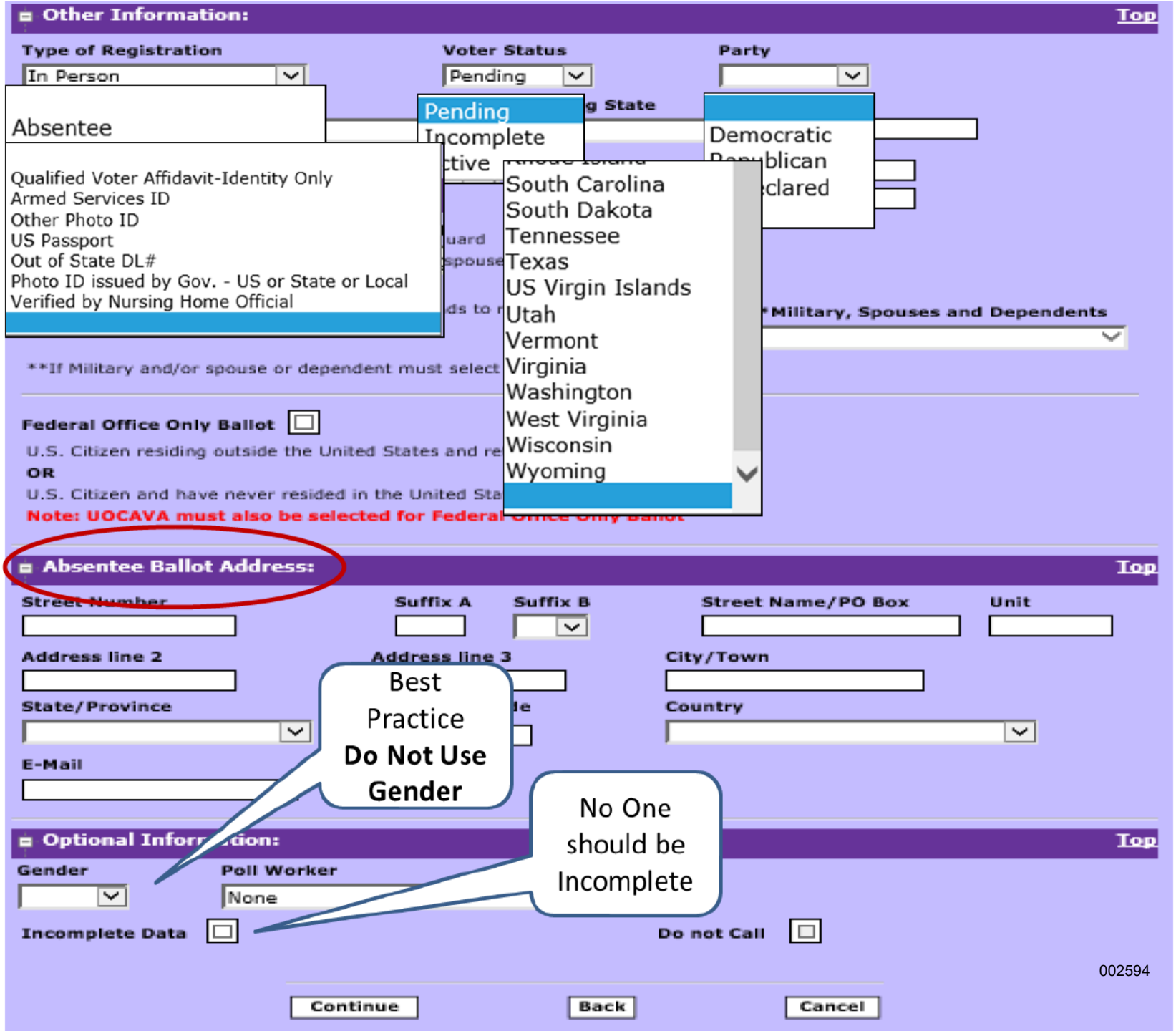
State/Province | Postal/Zip Code

Name under which previously registered if different:

Top

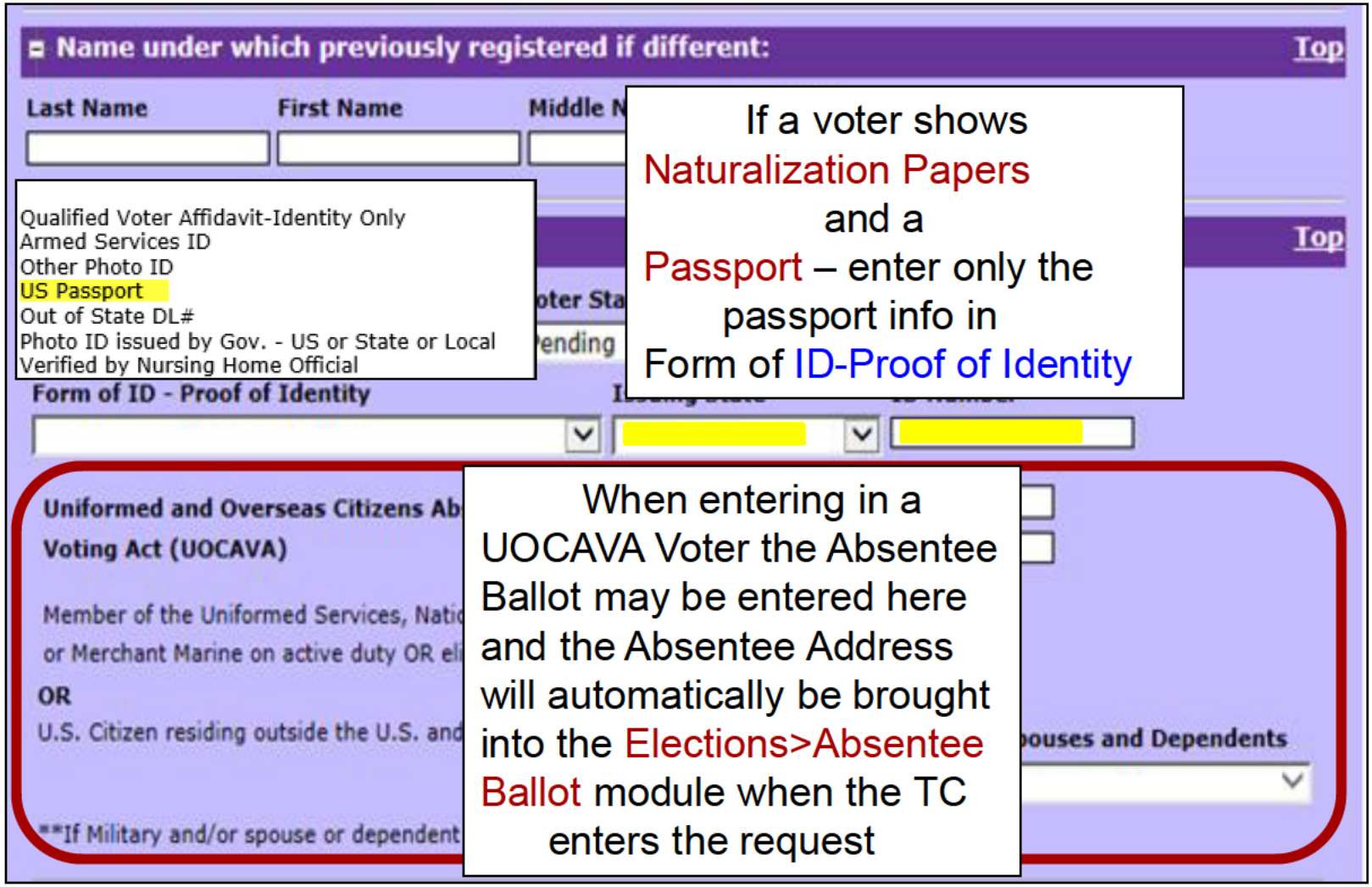
Last Name | First Name | Middle Name | Suffix

002593

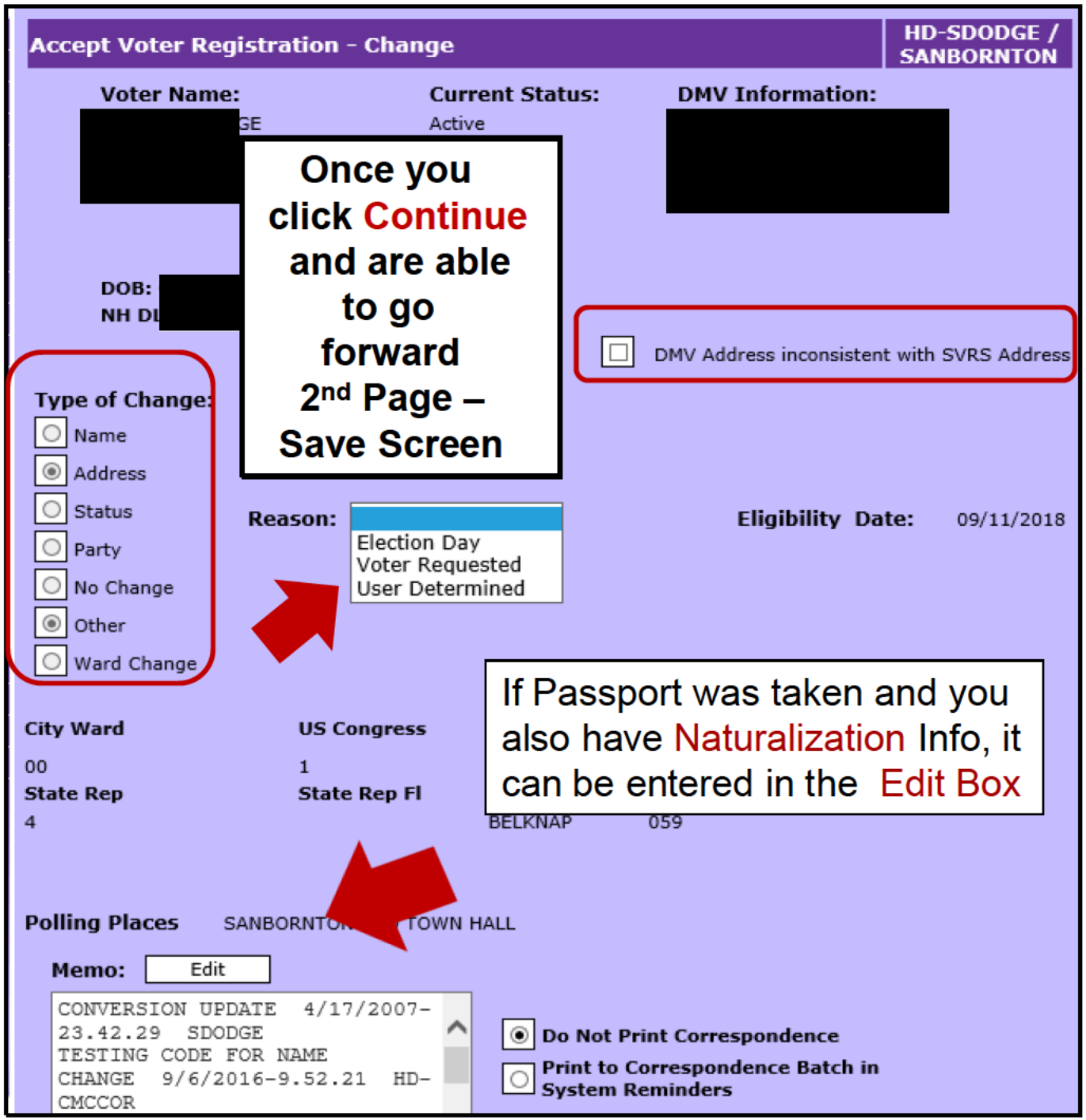

Other Information:
Top
Type of Registration
In Person
Absentee
Qualified Voter Affidavit-Identity Only
Armed Services ID
Other Photo ID
US Passport
Out of State DL#
Photo ID issued by Gov. - US or State or Local
Verified by Nursing Home Official
Voter Status
Pending
Pending
Incomplete
Party
Democratic
South Carolina
South Dakota
Tennessee
Texas
US Virgin Islands
Utah
Vermont
Virginia
Washington
West Virginia
Wisconsin
Wyoming
*Military, Spouses and Dependents
**If Military and/or spouse or dependent must select
Federal Office Only Ballot
U.S. Citizen residing outside the United States and re
OR
U.S. Citizen and have never resided in the United Sta
Note: UOCAVA must also be selected for Federal
Absentee Ballot Address:
Top
Street Number
Suffix A
Suffix B
Street Name/PO Box
Unit
Address line 2
Address line 3
City/Town
State/Province
Country
E-Mail
Best Practice Do Not Use Gender
No One should be Incomplete
Optional Information:
Top
Gender
Poll Worker
None
Incomplete Data
Do not Call
002594
Continue
Back
Cancel

Activities>Voter Registration>Add Change

WORK ZONE



002595



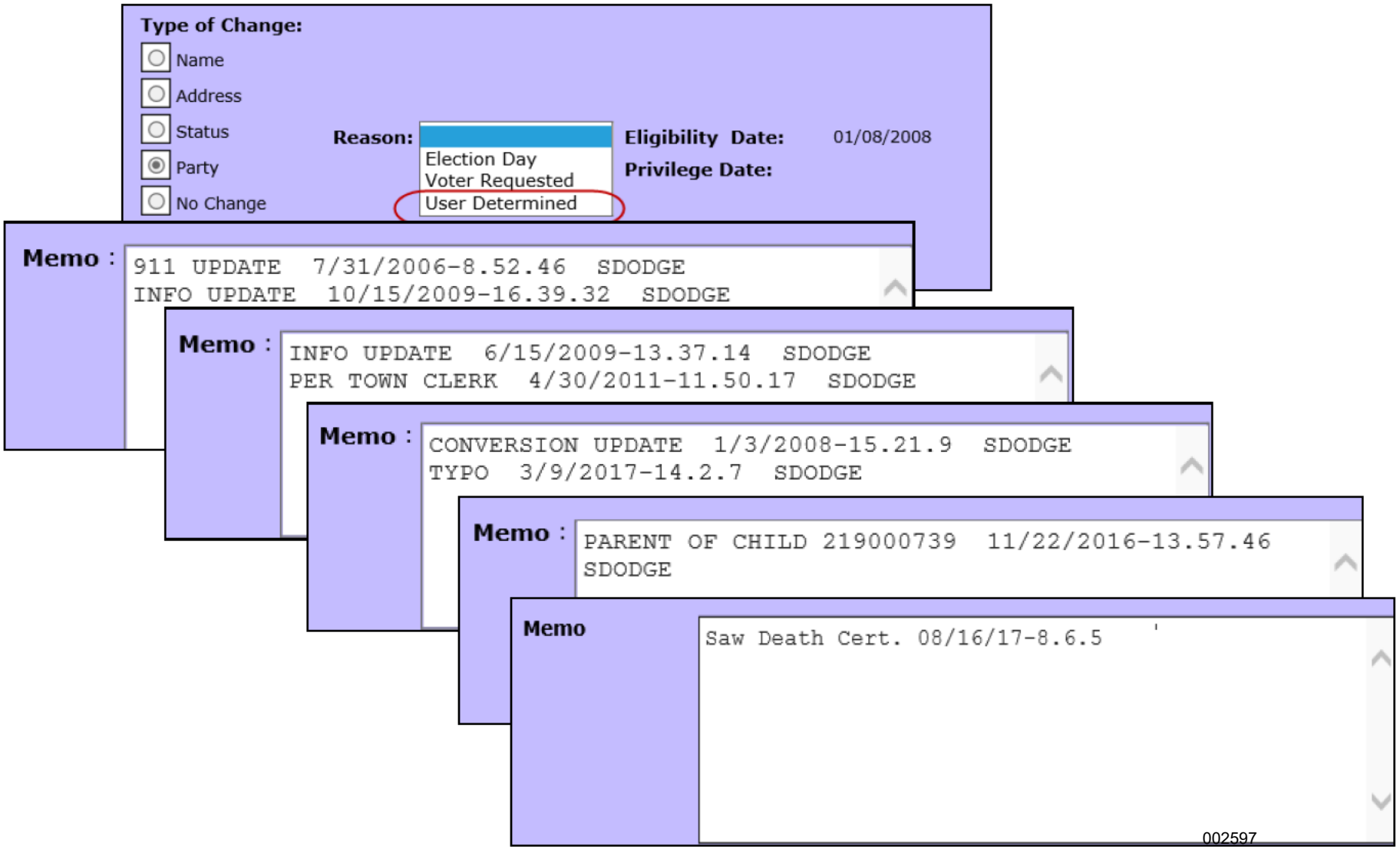
WORK ZONE

002596

Voter Registration MEMO BOX

WORK ZONE

When is it used?

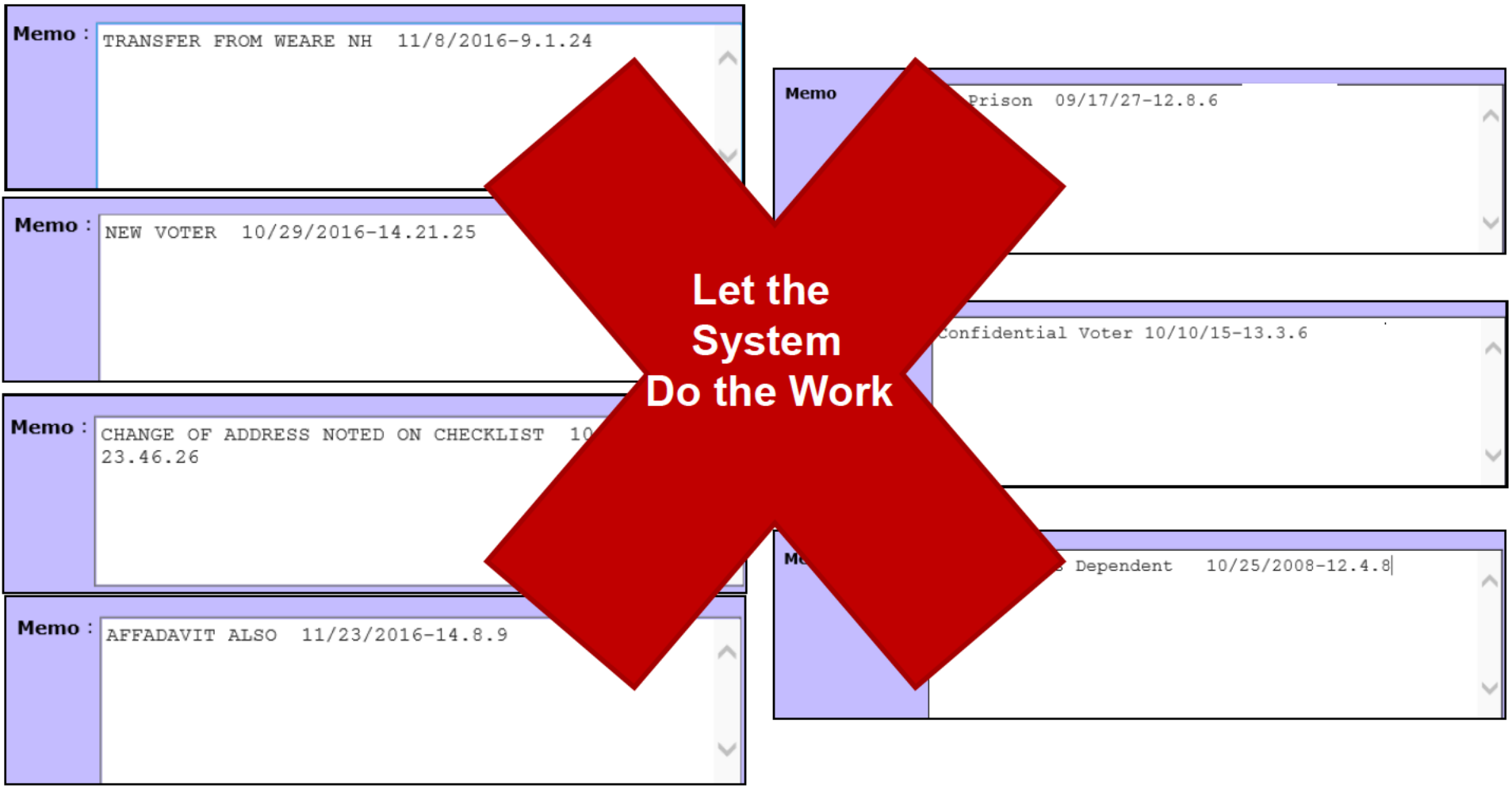


002597

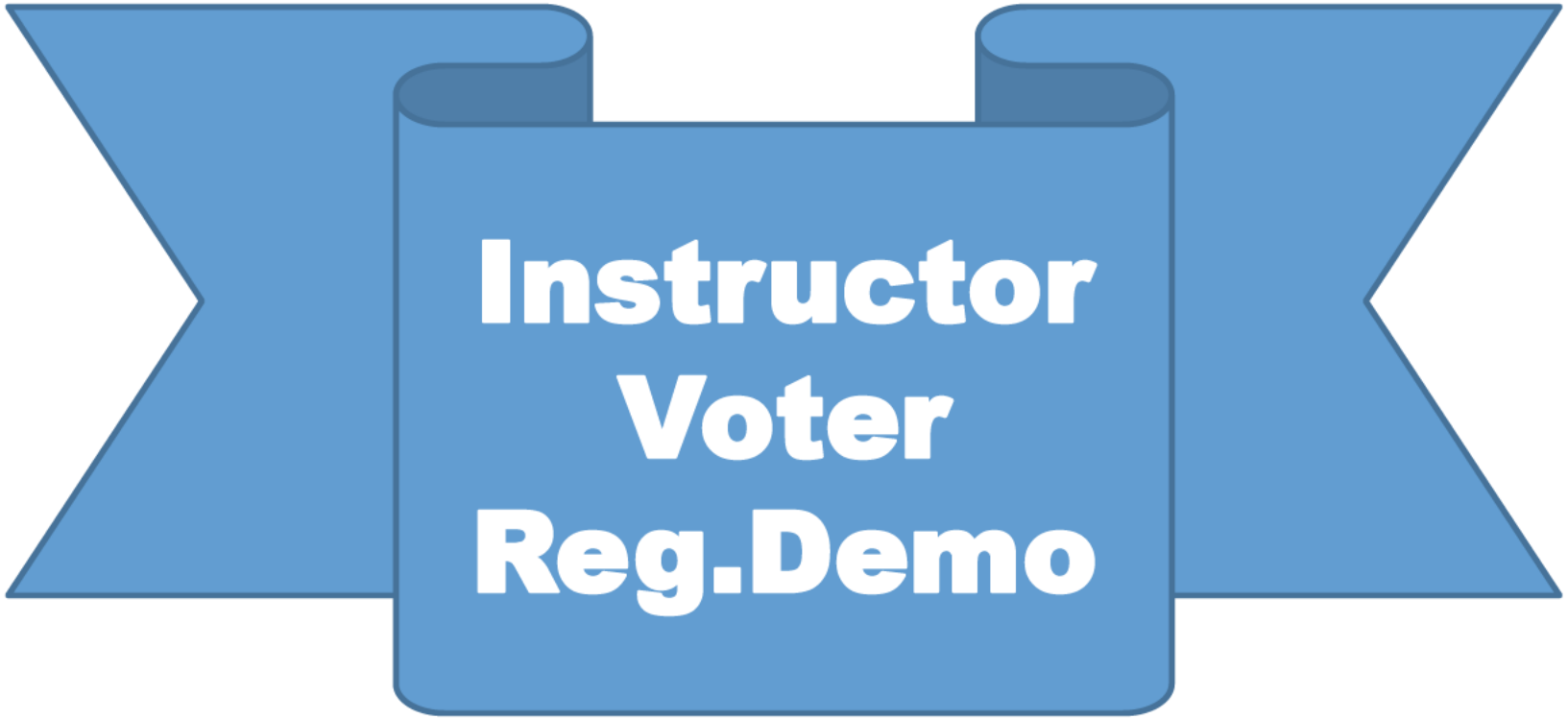
Voter Registration MEMO BOX

WORK ZONE

Examples of Information that does not need to be recorded



002598


Instructor
Voter
Reg.Demo

Chapter Review

WORK ZONE

Now that your voter is in the system – Where is his/her record?

On the Show **Reminder Screen** – Waiting for a Session in **Pending Approval**

What Status is the voter if entered as an Election Day Registration?

If the voter was entered as **EDR** in Type of Registration they are already **Active**

In either case where would you go to view the voters' information?

Inquiries> Help> Instructions

When does a new voter actually receive a Voter ID #?

Not until Save is click on the 2nd page of Voter Registration

When is it most appropriate to record something in the Edit Box?

When **USER DETERMINED** is the reason for altering the record

Absentee Ballots

WORK ZONE

Absentee Ballots are one of the Main Duties of the Town Clerks office at election time.

- The acceptance of an Absentee Ballot request
- Getting the Absentee Ballots out to the requestors
- The process of the Return of Absentee Ballots and getting them to the Polls
- The Data Entry in ElectioNet of Voters' Absentee Ballots
- Process for Absentee Ballots after the election

EPM – Absentee Ballot Info starts on page 37

Clerks – Absentee Forms & Instructions

Help->Instructions

2018 Election Law Changes Effective 1-1-2019
2018 General Election Process - Use for voters registered on or before November 6th 2018
2019 - Affidavit Envelope for Town or City
2019 - ElectioNet Updates - Absentee Ballot & Show Reminders
2019 - Town, Village District and School Elections Memo from SOS & AG
2019 Absentee Ballot Application - State
2019 Absentee Ballot Application - Town or City
30 Day Letter Process - 2017 v5
Absentee - Not Registered to Vote Package 2019-02
Absentee Ballot Insert - 2018 v3
Absentee Ballot Label Process - 2018
Absentee Ballot List - 2018
Absentee Ballot Mail Instructions for Primary or General 8-2018
Absentee Ballot Process - 2018
Absentee Ballot Processing on Election Day Memo
Absentee Ballot Rejected Reasons 11-2016
Absentee Ballot Requirements and Instructions 2018-09-20
Absentee Ballot Return Form 2019 - 2020

FPCA Flow Chart
FPCA Form - 2017

UOCAVA - Email Oval Primary or General Absentee Ballot Instructions
UOCAVA - Email Template
UOCAVA - FOO (Federal Office Only) Email Primary or General Absentee Ballot Instructions
UOCAVA - FOO (Federal Office Only) Mail Instructions for Primary or General
UOCAVA - How to Email an Absentee Ballot 2018
UOCAVA Check & Uncheck Instructions 2018
UOCAVA Oath - Affidavit Updated 2018-09-25
UOCAVA Return to Undeclared 2019

002602

Absentee Ballot – Classification

There are 2 types of absentee ballots:

Regular Absentee- those voters who are unable to make it to the Polls on election day

Uniformed and Overseas Citizens Absentee Voting Act

UOCAVA - those voters who are **Military** (Domestic or Overseas) **and Citizens** who are out of the country

Of the **UOCAVA** voters there are two subcategories which define what ballot they receive:

Full Ballot = All **Military and CitizensTemporarily Overseas**

Federal Office Only = **Citizens** not returning or don't know if they ever will return

002603

Absentee Ballot – Application

STATE OF NEW HAMPSHIRE
Application for State Election Absentee Ballot-RSA 657:4
Absence due to Religious Observance and Disability
(Uniformed and Overseas Citizen Voters Residing Outside the U.S. use the federal post card application)
http://sos.nh.gov/ElecForms2.aspx

For Official Use Only Voter Not registered ☐ Voter ID # _____ Date Returned: __/__/____ Date Mailed: __/__/____ Date Requested: __/__/____ Last Name: _____ First Name: _____

I. I hereby declare that (check one):
☐ I am a
☐ I am a
election,
necessary

II. I will
☐ I plan
where I a
☐ I am re
day of the
the date o
request 1
absent on
☐ I ca
commitme
☐ I am unable to vote in person due to a disability.
☐ I cannot appear at any time during polling hours at my polling place because of an employment obligation. For the purposes of this application, the term "employment" shall include the care of children and infirm adults, with or without compensation.

For use only on the Monday immediately prior to the election: I cannot appear at my polling place on election day because the National Weather Service has issued a winter storm warning, blizzard warning, or ice storm warning for election day applicable to my city, town, or unincorporated place and either (check one):
☐ I am elderly or infirm or I have a physical disability, and would otherwise vote in person but I have concerns for my safety traveling in the storm.
☐ I anticipate that school, child care, or adult care will be canceled, and would otherwise vote in person but will need to care for children or infirm adults.

Any person who votes or attempts to vote using an absentee ballot who is not entitled to vote by absentee ballot shall be guilty of a misdemeanor. RSA 657:24

III. I am requesting an official absentee ballot for the following election (check only one):
*Required for Primary Electi
affiliation with a party and I
only one):
☐ *Presidential Primary Election t
☐ Dem
☐ *State Primary Election to be he
☐ Democratic Party ☐ Republican Party
☐ State General Election to be held on November 3, 2020

Turn Over – You Must Complete the back side
Page 1 of 2

IV. Applicant's Name (Please Print):

Last Name First Name Middle Name (Jr., Sr., II,III)

Applicant's Voting Domicile (home) Address:

rd Zip Code

ress)

State Zip Code

day is preferred)

Applicant's Signature: _____ Date Signed: _____

The applicant must sign this form to receive an absentee ballot. Any person who witnesses and assists a voter with a disability in executing this form shall print and sign his or her name in the space provided on the application form.

I attest that I assisted the applicant in executing this form because he/she has a disability.

Signature _____ Print Name _____

Mail/fax/or hand deliver this completed form to your local City/Town Clerk.

For local clerk addresses and fax numbers: https://app.sos.nh.gov – Click on "Clerk Information Search" tab.

enteeBallot.aspx to track your absentee
btain the date when your absentee ballot
ompleted absentee ballot, and after the
t counted and why. Contact your clerk
he "Voter Information Look-up /

For Official Use Only:

Voter Verified ☐

002604

Page 2 of 2 1/19

Regular Absentee Request

Check to make sure the person is on your Checklist

If not they will need to register

2019 Absentee Ballot Application - State

2019 Absentee Ballot Application - Town or City

Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
Absentee Ballots
Select Default Election
Inquiry
Batch Returned

Search - Absentee Ballots | HD-SDODGE / MILFORD

OR

Voter Search Criteria:

Last Name | First Name | Middle Name | Voter ID

Legacy ID

Absentee Ballot | HD-SDODGE / SANBORNTON

Voter Information

Name	Date of Birth	Voter ID	Party	Ward
[redacted]	[redacted]	[redacted]	Republican	00

Residence Address [redacted] | License # | Legacy ID

Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ☑

UOCAVA Start Date

UOCAVA End Date 12 31 2019

Date You Received

Member of the Uniformed Services, National Guard or Merchant Marine on active duty OR eligible spouse or dependent

**If Military and/or spouse or dependent must select "Domestic" or "Overseas"

OR

U.S. Citizen residing outside the U.S. and intends to return

****Military, Spouses and Dependents**

Domestic (residing in the US)
Overseas (residing outside the US)

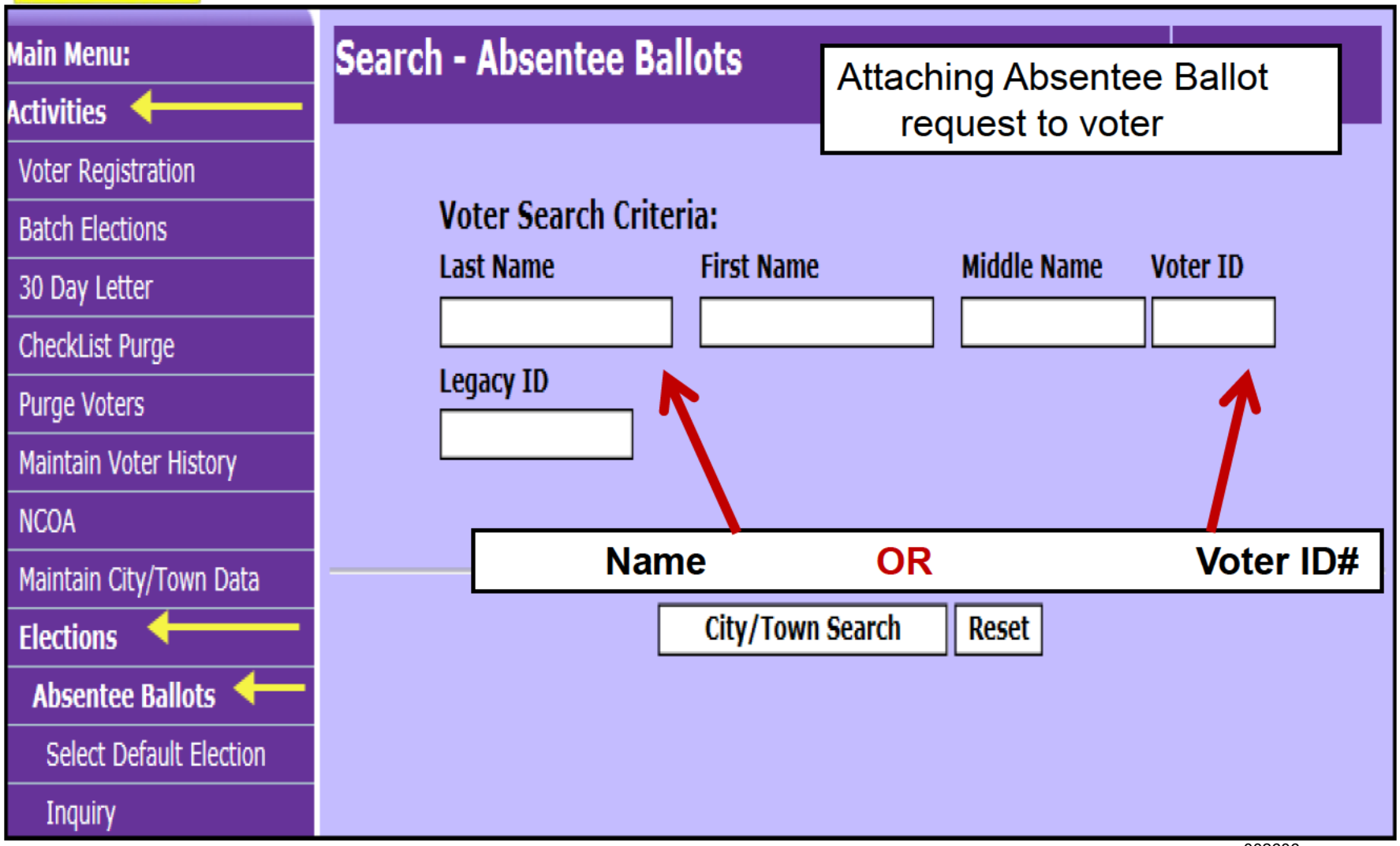
Save UOCAVA Voter Information

Absentee Ballots: There are no Absentee Ballots for this Voter

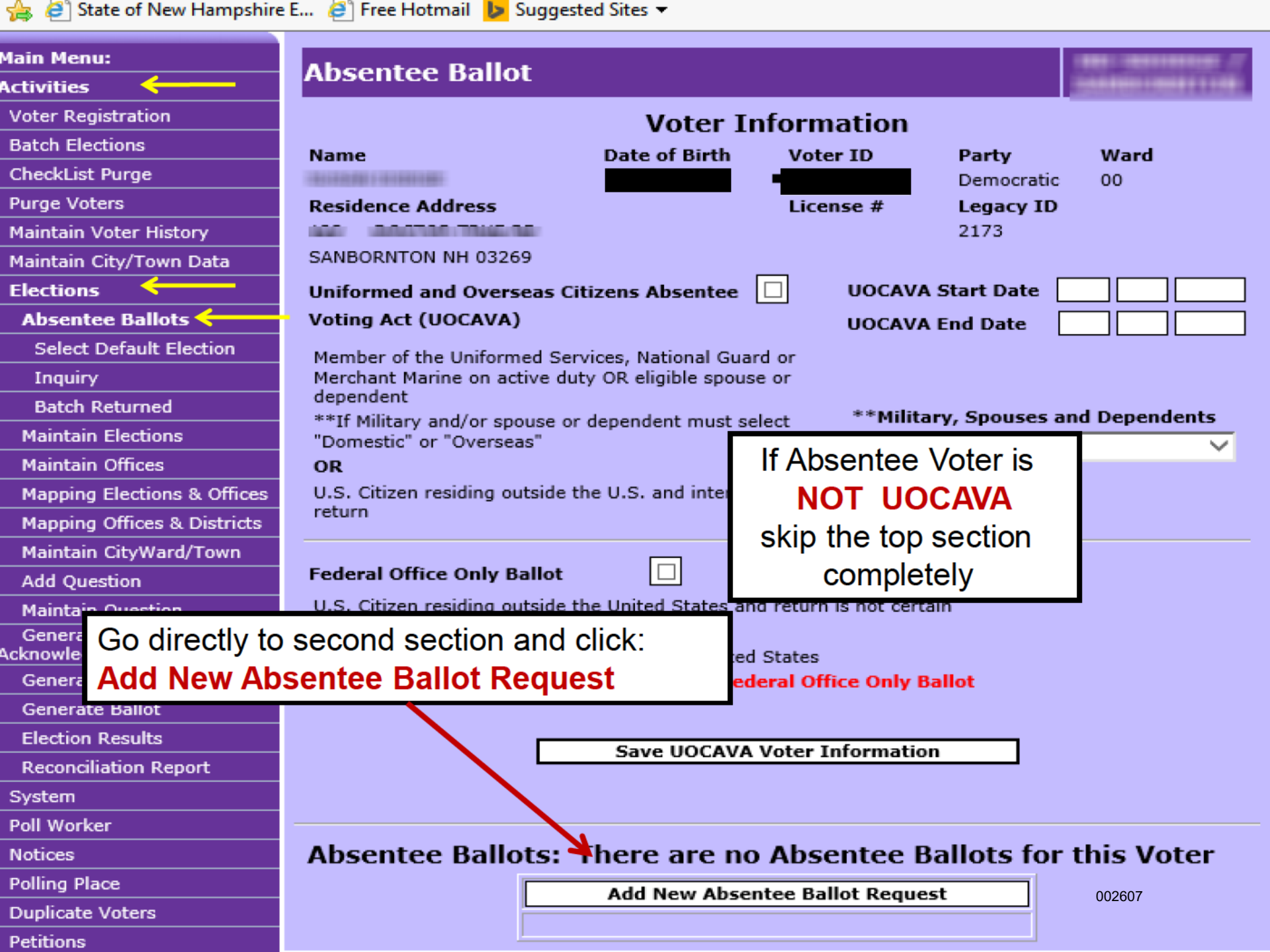
Add New Absentee Ballot Request

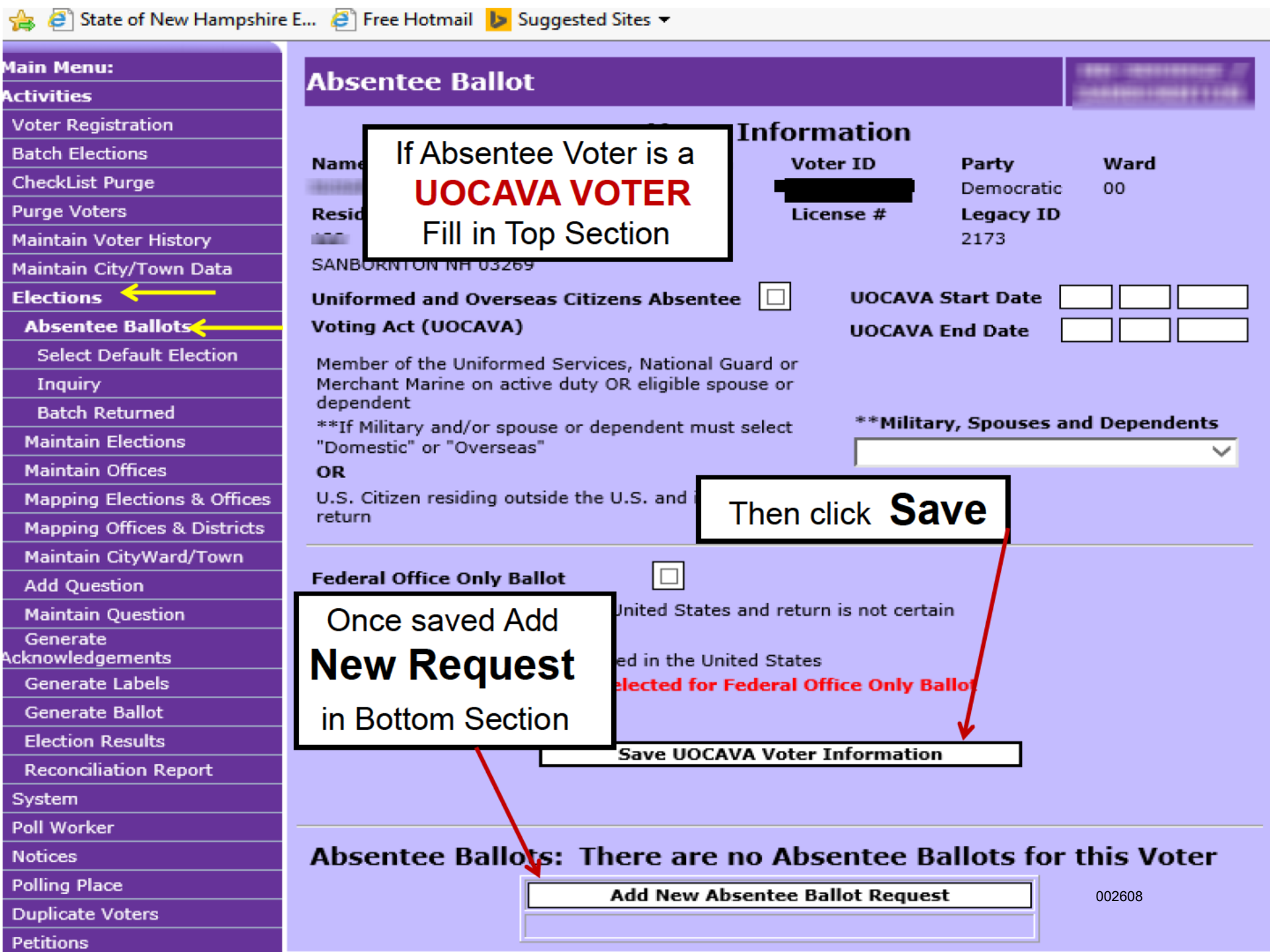
002605

Absentee Ballot – Search Name



002606


State of New Hampshire E...
Free Hotmail
Suggested Sites
Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
Absentee Ballots
Select Default Election
Inquiry
Batch Returned
Maintain Elections
Maintain Offices
Mapping Elections & Offices
Mapping Offices & Districts
Maintain CityWard/Town
Add Question
Maintain Question
Generate Ballot
Election Results
Reconciliation Report
System
Poll Worker
Notices
Polling Place
Duplicate Voters
Petitions
Absentee Ballot
Voter Information
Name
Date of Birth
Voter ID
Party
Democratic
Ward
00
Residence Address
License #
Legacy ID
2173
SANBORNTON NH 03269
Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)
UOCAVA Start Date
UOCAVA End Date
Member of the Uniformed Services, National Guard or Merchant Marine on active duty OR eligible spouse or dependent
**If Military and/or spouse or dependent must select "Domestic" or "Overseas"
OR
U.S. Citizen residing outside the U.S. and inte
return
**Military, Spouses and Dependents
If Absentee Voter is NOT UOCAVA skip the top section completely
Federal Office Only Ballot
U.S. Citizen residing outside the United States and return is not certain
ed States
ederal Office Only Ballot
Go directly to second section and click:
Add New Absentee Ballot Request
Save UOCAVA Voter Information
Absentee Ballots: There are no Absentee Ballots for this Voter
Add New Absentee Ballot Request
002607


State of New Hampshire E...
Free Hotmail
Suggested Sites
Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
Absentee Ballots
Select Default Election
Inquiry
Batch Returned
Maintain Elections
Maintain Offices
Mapping Elections & Offices
Mapping Offices & Districts
Maintain CityWard/Town
Add Question
Maintain Question
Generate Acknowledgements
Generate Labels
Generate Ballot
Election Results
Reconciliation Report
System
Poll Worker
Notices
Polling Place
Duplicate Voters
Petitions
Absentee Ballot
Information
If Absentee Voter is a
UOCAVA VOTER
Fill in Top Section
Voter ID
Party
Democratic
Ward
00
License #
Legacy ID
2173
SANBORNTON NH 03269
Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)
UOCAVA Start Date
UOCAVA End Date
Member of the Uniformed Services, National Guard or Merchant Marine on active duty OR eligible spouse or dependent
**If Military and/or spouse or dependent must select "Domestic" or "Overseas"
OR
U.S. Citizen residing outside the U.S. and
return
**Military, Spouses and Dependents
Then click Save
Federal Office Only Ballot
United States and return is not certain
ed in the United States
elected for Federal Office Only Ballot
Once saved Add
New Request
in Bottom Section
Save UOCAVA Voter Information
Absentee Ballots: There are no Absentee Ballots for this Voter
Add New Absentee Ballot Request
002608

ADD NEW ABSENTEE BALLOT

Don't For-Get to click Save at bottom of page

Main Menu:
Activities
Voter Registration
Batch Elections
CheckList Purge
Purge Voters
Maintain Voter History
Maintain City/Town Data
Elections
Absentee Ballots
Maintain Elections
Maintain Offices
Mapping Elections & Offices
Mapping Offices & Districts
Maintain CityWard/Town
Add Question
Maintain Question
Generate Acknowledgements
Generate Labels
Generate Ballot
Election Results
Reconciliation Report
System
Poll Worker
Notices
Polling Place
Duplicate Voters
Petitions
Candidate Management
State Archive
Reports
Inquiries
Help
Logout

ElectioNet
Service and Information ... Reformed

Add Absentee Ballots | HD-SDODGE / SANBORNTON

Name | Date of Birth | Voter ID | Party: Republican | Ward: 00
Residence Address | License # | Legacy ID | UOCAVA Start | UOCAVA End

Election Date -- Name
03/12/2019--SANBORNTON TOWN ELECTION
11/06/2018--STATE GENERAL ELECTION
09/11/2018--STATE PRIMARY ELECTION
03/13/2018--SANBORNTON TOWN ELECTION
03/15/2017--SANBORNTON TOWN MEETING

Date Requested: 02 08 2019
Request Type: Email Facsimile / Facsimile / In-Person / Mail
Military, Spouses and Dependents: Domestic (residing in the US) / Overseas (residing outside the US)
Memo
Date Mailed/E-Mailed/Handed to Voter
REP

Ballot Mailing Address:
- Use the Domicile Address / Handed to Voter
- Use the Mailing Address
- Use the Absentee Ballot Address
- Use the Absentee Ballot E-Mail

Street Number | Suffix A | Suffix B | Street Name/PO Box | Unit
Address Line 2 | Address Line 3 | City
State: New Hampshire | Country: United States | Postal/Zip Code
E-Mail

Update the Absentee Ballot Record in the Voter Record

NEW

Ballot Return Information:
Date Ballot Returned
Check Only if a Federal Write-in Absentee Ballot (FWAB) was returned
Voter Verified:

Ballot Returned Undeliverable
Rejected
Challenged
Reject Reasons
Challenge Reason
Challenged By

Save Reset

Applications & Affidavit Envelopes

- Absentee Ballot – applications and affidavit envelopes (RSA 659:50, III):
  - ✓ If a voter with a disability receives assistance in executing the *application form* **or** *the affidavit envelope*, that person assisting shall make a statement on the form and the affidavit acknowledging that assistance was provided;
  - ✓ State **Absentee Ballot Application** can be found on the SOS website or **Election*Net* -> Help -> Instructions**

New Absentee Verbiage

Absentee Application

Applicant's Signature: _____ Date Signed: _____

The applicant must sign this form to receive an absentee ballot. Any person who witnesses and assists a voter with a disability in executing this form shall print and sign his or her name in the s

I attest that I ... ability.

Signature _____

I am voting on the Monday immediately prior to the election, the National Weather Service has issued a winter storm warning, blizzard warning, or ice storm warning, and I am elderly or infirm, have a physical disability, or have to care for children or infirm adults,

rn Envelope

Absence from City or To ... **ability**. A person voting by from the city or town in ... disability shall fill out and following certificate: I do ... penalties for voting fraud below that I am a voter in ... of _____, New ward ___; that I will be un... mmitment which prevents place because I will be working on election day or I am voting ... or that on account of physical disability I am unable to vote in immediately prior to the election, the National Weather Service ha... storm warning, blizzard warning, or ice storm warning, and I am elder... a physical disability, or have to care for children or infirm adults, or I... absent on election day from said city or town and will be unable to v...

I certify that I have carefully read (or had read to me because I am blin... allot herein enclosed, and that I personally marked the ballot within and sealed it in this envelope (or had assistance in marking th... se I am blind).

Signature _____

Print Name _____

A person assisting a disabled or blind voter shall make and sign a s... ded acknowledging the assistance.

I attest that I assisted the applicant in executing this form be...

Signature _____ Print Name _____

In accordance with RSA 659:34, the penalty for knowingly or purposely providing false information when registering to vote or voting is a class A misdemeanor with a maximum sentence of imprisonment not to exceed one year and a fine not to exceed $2,000. Fraudulently registering to vote or voting is subject to a civil penalty not to exceed $5,000.

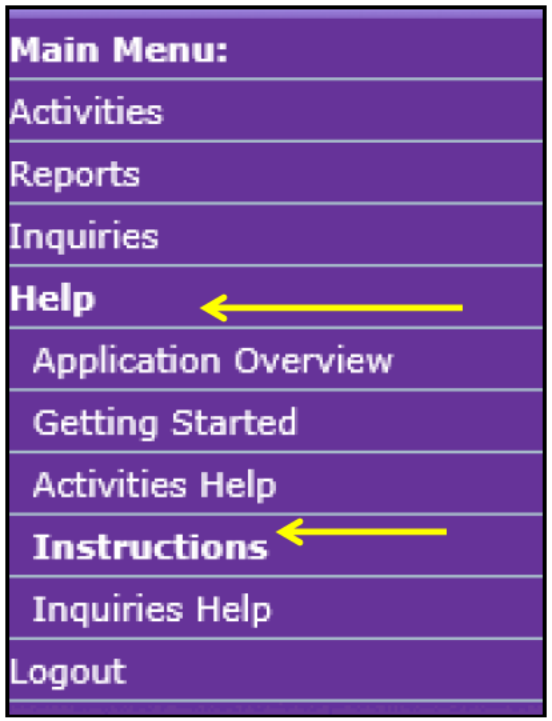
Form A 1/2019

Towns are responsible for printing their **Local Election Envelopes**

Absentee Ballot – Return Form

Absentee Return Form

RSA 657:17



STATE OF NEW HAMPSHIRE
Absentee Ballot Return Form
(RSA 657:17)
To be completed by the person who is returning an Absentee Ballot for someone *other than themselves*
[illegible] or Disability

For Official Use Only
Voter Not registered ☐
Voter ID #: _____

I. I hereby declare that I am the voter's (check one):

☐ Spouse ☐ Parent ☐ Sibling ☐ Child

Any person who votes or attempts to vote using an absentee ballot who is not entitled to vote by absentee ballot shall be guilty of a misdemeanor. RSA 657:24

II. Absentee Ballot Voter's Name (Please Print):

Last Name First Name Middle Name (Jr., Sr., II, III)

Absentee Ballot Voter's Domicile (home) Address:

Street Number Street Name Apt/Unit City/Town Ward Zip Code

Date Returned: ___/___/_____

III. Name of family member who delivered the absentee ballot (Please Print):

Last Name First Name Middle Name (Jr., Sr., II, III)

Signature:_____ Date Signed_____

IV. Election Name (check only one and enter date):

☐ Town/ City Election Date:____/____/_____
☐ State Special Primary Election Date:____/____/_____
☐ State Special General Election Date:____/____/_____
☐ Presidential Primary Date:____/____/_____
☐ State Primary Election Date: 09/08/2020
☐ State General Election Date: 11/03/2020

V. Proof of Identification (check only one):

☐ Government-issued Photo ID
☐ Identity verified by city or town clerk

VI. City or Town Clerk signature:

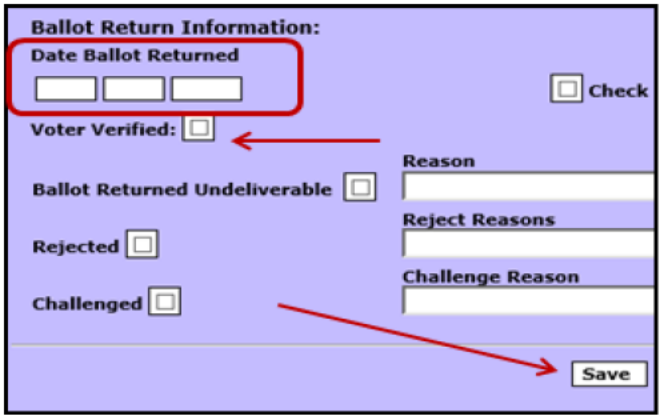
Printed Name of Clerk: _____

Clerk's Signature:_____ Date Signed: _____

002612

2019 v3

Verification of In-Person Absentee Ballot
Effective 01-01-2019
RSA 657:17-a



NEW

Voter Verified

- Upon Return of Absentee -

☐ Examine any photo identification offered to ensure it matches the voter and meets the requirements of RSA 659:13;

• If the voter does not have photo identification or prefers, the voter may voluntarily complete the challenged voter affidavit form. If the camera used on election day is available, the clerk should take the voter's photo and attach it to the affidavit. A photo is not taken if the camera is not available or if the voter has a religious objection to being photographed. The clerk must sign the bottom of the challenged voter affidavit attesting that the voter took the oath and is the person that signed the affidavit.

2019 - ElectioNet Updates - Absentee Ballot & Show Reminders

002613

Absentee Ballot – Returned Voter

Save UOCAVA Voter Information

Absentee Ballots

Add New Absentee Ballot Request

Select	Date Requested	Date Mailed	Date Returned	Election Date	Election Type, Category
○	02/11/2019	02/11/2019		05/15/2019	Primary, State

☐ Print Bar Code on Mailing Label

Delete | Update | Generate Mailing Label | Display Signature

Instance : UAT Instance2 - ©2018 PCC Technology INC. All rights reserved.

Select Election

Update

Main Menu:

- **Activities** ←
  - Voter Registration
  - Batch Elections
  - CheckList Purge
  - Purge Voters
  - Maintain Voter History
  - Maintain City/Town Data
- **Elections** ←
  - **Absentee Ballots** ←

Ballot Return Information:

Date Ballot Returned: 02 / 11 / 2019

Enter Date of Return

☐ Check Only if a Federal Write-in Absentee Ballot (FWAB) was returned

Voter Verified: ☑

Ballot Returned Undeliverable ☐ Reason

Rejected ☐ ect Reasons

Challenged ☐ llenge Reason Challenged By

If voter was **Verified** check box

Save | Reset

002614

Absentee Ballot – Reports

Main Menu:
- Activities
- Reports
- Report Status
- Absentee Ballots
- Challenges
- List
- Mailing Labels
- More Than One Returned
- Returned Undeliverable
- Rejected
- UOCAVA Rejected
- UOCAVA Summary
- UOCAVA Summary Cast
- City/Town Data
- Elections
- Statewide
- System
- Voters
- Inquiries
- Help
- Logout

ElectioNet Service and Information ... Reformed

Absentee Ballots

Town/City Wards | State Senatorial | State Rep | Executive Council | County | School | Village Districts

Wards/Districts: none

Party: Democratic, Republican, Undeclared

Voter Status: Active, Incomplete, Pending, Pending Removal

Ballot Type: Domestic (residing in the US), Overseas (residing outside the US)

UOCAVA Only ☐

Include Verified Voter: ☑

Print Absentee Mailing Address ☐

Include Confidentiality Program Voters ☐

Date Requested | Date Mailed | Date Returned | Not Returned

Start Date : / /

End Date : / /

Election Date -- Name: 03/12/2019-- TOWN ELECTION

Election Type: General

Election Category: Town/City Election

Last Name Range(Alpha): From: A To: Z

Age Range: From: To:

Report Generation Options:

Generation Type: PDF

Submit Request | Reset

Reports/Absentee Ballots

Help/Instructions

Absentee Ballot Process

- Absentee Ballot Process - 2019
- Absentee Ballot Processing on Election Day Memo
- Absentee Ballot Report List - 2019

Absentee Ballot – List

02/11/2019 — Absentee Ballot - Statewide — Page 2

Ward :- 00

Voter ID	Voter Name	Residence Address	Ward	Party	UND Bal. Ch.	Date Requested	Date Mailed	Date Returned	Generated Verified Voter	UOCAVA	FOO
300447086	[redacted]	[redacted]	00	UND	DEM	01/17/2019	01/17/2019	01/17/2019			
300067427	[redacted]		00	UND	REP	01/17/2019	01/17/2019	01/17/2019	X		
300233339	[redacted]		00	DEM	DEM	01/01/2019	01/01/2019	01/15/2019			
164000011	[redacted]		00	DEM	DEM	01/17/2019	01/17/2019	01/17/2019			
237001310	[redacted]		00	DEM	DEM	01/01/2019	01/01/2019	01/15/2019			
237000080	[redacted]		00	DEM	DEM	01/17/2019	01/17/2019	01/17/2019			
209000155	[redacted]		00	DEM	DEM	01/17/2019	01/17/2019	01/17/2019			
129000486	[redacted]		00	REP	REP	02/06/2019	02/06/2019			X	
209000127	[redacted]		00	DEM	DEM	02/06/2019	02/06/2019			X	X
300324581	[redacted]		00	UND	REP	02/06/2019	02/06/2019				
209000435	[redacted]		00	REP	REP	02/01/2019	02/06/2019				
209000437	[redacted]		00	UND	DEM	02/06/2019	02/06/2019	02/06/2019		X	
209000963	[redacted]		00	REP	REP	02/11/2019	02/11/2019		X		

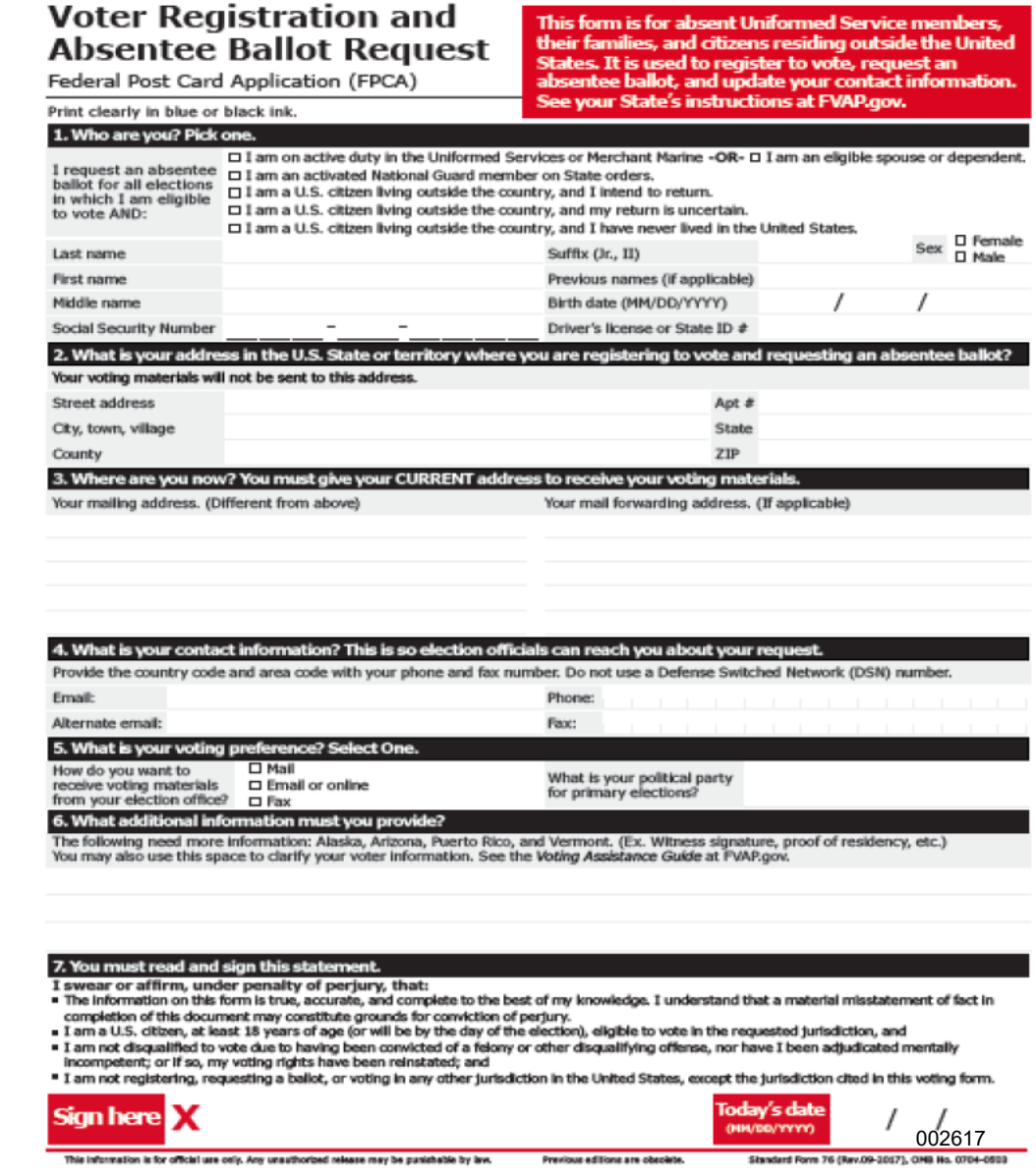
Total Count for ward 00 : 13 | 13 | 8

Absentee Ballot – UOCAVA

FPCA

Federal
Post
Card
Application

Uniformed (& or)
Overseas
Citizen
Absentee
Voter
Act



Voter Registration and Absentee Ballot Request

Federal Post Card Application (FPCA)

This form is for absent Uniformed Service members, their families, and citizens residing outside the United States. It is used to register to vote, request an absentee ballot, and update your contact information. See your State's instructions at FVAP.gov.

Print clearly in blue or black ink.

1. Who are you? Pick one.

I request an absentee ballot for all elections in which I am eligible to vote AND:

- ☐ I am on active duty in the Uniformed Services or Merchant Marine -OR- ☐ I am an eligible spouse or dependent.
- ☐ I am an activated National Guard member on State orders.
- ☐ I am a U.S. citizen living outside the country, and I intend to return.
- ☐ I am a U.S. citizen living outside the country, and my return is uncertain.
- ☐ I am a U.S. citizen living outside the country, and I have never lived in the United States.

Last name		Suffix (Jr., II)	Sex ☐ Female ☐ Male
First name		Previous names (if applicable)	
Middle name		Birth date (MM/DD/YYYY)	/ /
Social Security Number	___ ___ ___ - ___ ___ - ___ ___ ___ ___	Driver's license or State ID #	

2. What is your address in the U.S. State or territory where you are registering to vote and requesting an absentee ballot?

Your voting materials will not be sent to this address.

Street address		Apt #	
City, town, village		State	
County		ZIP	

3. Where are you now? You must give your CURRENT address to receive your voting materials.

Your mailing address. (Different from above)	Your mail forwarding address. (If applicable)

4. What is your contact information? This is so election officials can reach you about your request.

Provide the country code and area code with your phone and fax number. Do not use a Defense Switched Network (DSN) number.

Email:		Phone:	
Alternate email:		Fax:	

5. What is your voting preference? Select One.

How do you want to receive voting materials from your election office?	☐ Mail ☐ Email or online ☐ Fax	What is your political party for primary elections?

6. What additional information must you provide?

The following need more information: Alaska, Arizona, Puerto Rico, and Vermont. (Ex. Witness signature, proof of residency, etc.)
You may also use this space to clarify your voter information. See the *Voting Assistance Guide* at FVAP.gov.

7. You must read and sign this statement.

I swear or affirm, under penalty of perjury, that:

- The information on this form is true, accurate, and complete to the best of my knowledge. I understand that a material misstatement of fact in completion of this document may constitute grounds for conviction of perjury.
- I am a U.S. citizen, at least 18 years of age (or will be by the day of the election), eligible to vote in the requested jurisdiction, and
- I am not disqualified to vote due to having been convicted of a felony or other disqualifying offense, nor have I been adjudicated mentally incompetent; or if so, my voting rights have been reinstated; and
- I am not registering, requesting a ballot, or voting in any other jurisdiction in the United States, except the jurisdiction cited in this voting form.

Sign here X

Today's date (MM/DD/YYYY) / /

002617

This information is for official use only. Any unauthorized release may be punishable by law. Previous editions are obsolete. Standard Form 76 (Rev.09-2017), OMB No. 0704-0503

Absentee Ballot – UOCAVA

FPCA

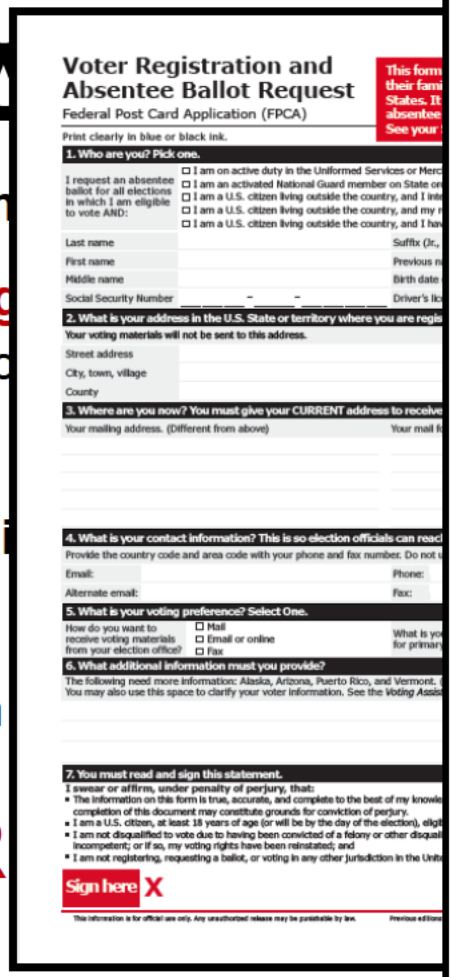
This is a request for an

It is used as a voter **Reg**
Form if the person is no
in your town.

There is no **"Place of Bi**
Application.

The **Place of Birth**

BEAN'S GR



Voter Registration and Absentee Ballot Request

Federal Post Card Application (FPCA)

Print clearly in blue or black ink.

1. Who are you? Pick one.

I request an absentee ballot for all elections in which I am eligible to vote AND:

☐ I am on active duty in the Uniformed Services or Merc
☐ I am an activated National Guard member on State or
☐ I am a U.S. citizen living outside the country, and I int
☐ I am a U.S. citizen living outside the country, and my r
☐ I am a U.S. citizen living outside the country, and I hav

Last name | Suffix (Jr., | First name | Previous n | Middle name | Birth date | Social Security Number | Driver's lic

2. What is your address in the U.S. State or territory where you are regis

Your voting materials will not be sent to this address.

Street address | City, town, village | County

3. Where are you now? You must give your CURRENT address to receive

Your mailing address. (Different from above) | Your mail fo

4. What is your contact information? This is so election officials can reac

Provide the country code and area code with your phone and fax number. Do not u

Email: | Phone: | Alternate email: | Fax:

5. What is your voting preference? Select One.

How do you want to receive voting materials from your election office? ☐ Mail ☐ Email or online ☐ Fax | What is yo for primary

6. What additional information must you provide?

The following need more information: Alaska, Arizona, Puerto Rico, and Vermont.
You may also use this space to clarify your voter information. See the Voting Assis

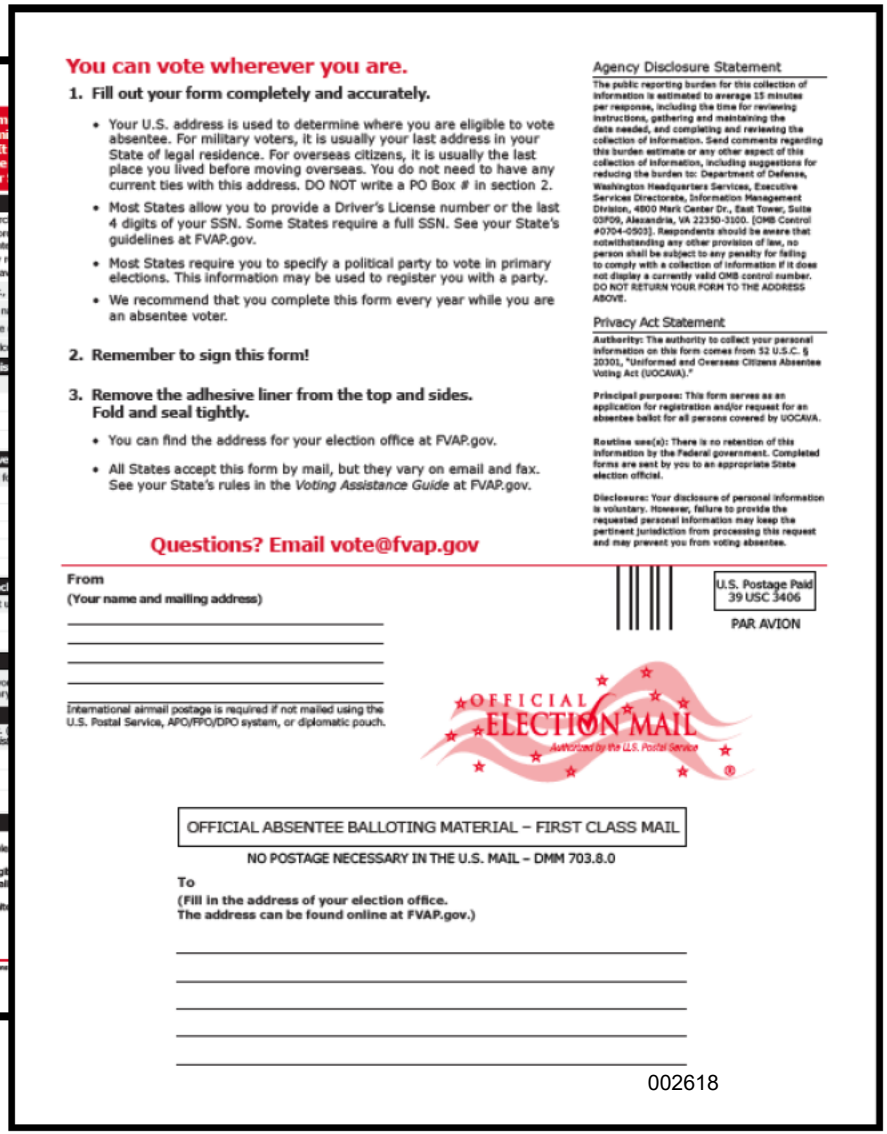
7. You must read and sign this statement.

I swear or affirm, under penalty of perjury, that:

- The information on this form is true, accurate, and complete to the best of my knowle completion of this document may constitute grounds for conviction of perjury.
- I am a U.S. citizen, at least 18 years of age (or will be by the day of the election), eligi
- I am not disqualified to vote due to having been convicted of a felony or other disqual incompetent; or if so, my voting rights have been reinstated; and
- I am not registering, requesting a ballot, or voting in any other jurisdiction in the Unit

Sign here X

This information is for official use only. Any unauthorized release may be punishable by law. Previous edition



You can vote wherever you are.

1. **Fill out your form completely and accurately.**
   - Your U.S. address is used to determine where you are eligible to vote absentee. For military voters, it is usually your last address in your State of legal residence. For overseas citizens, it is usually the last place you lived before moving overseas. You do not need to have any current ties with this address. DO NOT write a PO Box # in section 2.
   - Most States allow you to provide a Driver's License number or the last 4 digits of your SSN. Some States require a full SSN. See your State's guidelines at FVAP.gov.
   - Most States require you to specify a political party to vote in primary elections. This information may be used to register you with a party.
   - We recommend that you complete this form every year while you are an absentee voter.
2. **Remember to sign this form!**
3. **Remove the adhesive liner from the top and sides. Fold and seal tightly.**
   - You can find the address for your election office at FVAP.gov.
   - All States accept this form by mail, but they vary on email and fax. See your State's rules in the *Voting Assistance Guide* at FVAP.gov.

Questions? Email vote@fvap.gov

Agency Disclosure Statement

The public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden to: Department of Defense, Washington Headquarters Services, Executive Services Directorate, Information Management Division, 4800 Mark Center Dr., East Tower, Suite 03F09, Alexandria, VA 22350-3100. [OMB Control #0704-0503]. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. DO NOT RETURN YOUR FORM TO THE ADDRESS ABOVE.

Privacy Act Statement

Authority: The authority to collect your personal information on this form comes from 52 U.S.C. § 20301, "Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)."

Principal purpose: This form serves as an application for registration and/or request for an absentee ballot for all persons covered by UOCAVA.

Routine use(s): There is no retention of this information by the Federal government. Completed forms are sent by you to an appropriate State election official.

Disclosure: Your disclosure of personal information is voluntary. However, failure to provide the requested personal information may keep the pertinent jurisdiction from processing this request and may prevent you from voting absentee.

From
(Your name and mailing address)

U.S. Postage Paid
39 USC 3406

PAR AVION

International airmail postage is required if not mailed using the U.S. Postal Service, APO/FPO/DPO system, or diplomatic pouch.

OFFICIAL ELECTION MAIL
Authorized by the U.S. Postal Service

OFFICIAL ABSENTEE BALLOTING MATERIAL – FIRST CLASS MAIL

NO POSTAGE NECESSARY IN THE U.S. MAIL – DMM 703.8.0

To
(Fill in the address of your election office.
The address can be found online at FVAP.gov.)

002618

Voter Registration and Absentee Ballot Request

Federal Post Card Application (FPCA)

Print clearly in blue or black ink.

This form is for absent Uniformed Service members, their families, and citizens residing outside the United States. It is used to register to vote, request an absentee ballot, and update your contact information. See your State's instructions at FVAP.gov.

1. Who are you? Pick one.

I request an absentee ballot for all elections in which I am eligible to vote AND:

- ☐ I am on active duty in the Uniformed Services or Merchant Marine **-OR-** ☐ I am an eligible spouse or dependent.
- ☐ I am an activated National Guard member on State orders.
- ☐ I am a U.S. citizen living outside the country, and I intend to return.
- ☐ I am a U.S. citizen living outside the country, and my return is uncertain.
- ☐ I am a U.S. citizen living outside the country, and I have never lived in the United States.

✓

If one of the **first three** choices is checked in **Section One** by the applicant they are eligible to receive a **Full Ballot**.

✓

If either of the **last two** are checked they are eligible for the **FOO Ballot.**

002619

Absentee Ballot – UOCAVA

7. You must read and sign this statement.

I swear or affirm, under penalty of perjury, that:

- The information on this form is true, accurate, and complete to the best of my knowledge. I understand that a material misstatement of fact in completion of this document may constitute grounds for conviction of perjury.
- I am a U.S. citizen, at least 18 years of age (or will be by the day of the election), eligible to vote in the requested jurisdiction, and
- I am not disqualified to vote due to having been convicted of a felony or other disqualifying offense, nor have I been adjudicated mentally incompetent; or if so, my voting rights have been reinstated; and
- I am not registering, requesting a ballot, or voting in any other jurisdiction in the United States, except the jurisdiction cited in this voting form.

Sign here X [redacted] **Today's date (MM/DD/YYYY)** 03/01/2019

This information is for official use only. Any unauthorized release may be punishable by law. Previous editions are obsolete. Standard Form 76 (Rev.09-2017), OMB No. 0704-0503

Electronic Signature can not be accepted

Must be <u>signed</u> by Applicant

002620

[redacted]

2020 45 Day Deadline

Elections are noted in Green State Primary September 8, 2020, General Election November 3, 2020
45 Day Deadlines are noted in Red July 25, 2020 Saturday, September 19, 2020 Saturday

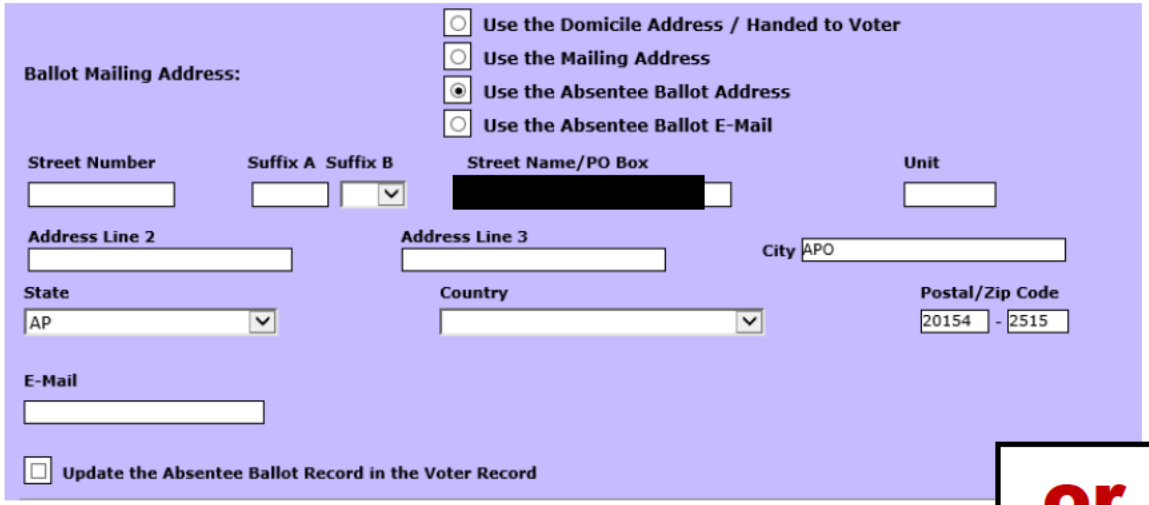
Do Not wait for the 45 Day Deadline to mail out UOCAVA ballots.

As soon as you receive the UOCAVA ballots you need to start sending them out

002621

Absentee Ballot – UOCAVA

Mail?

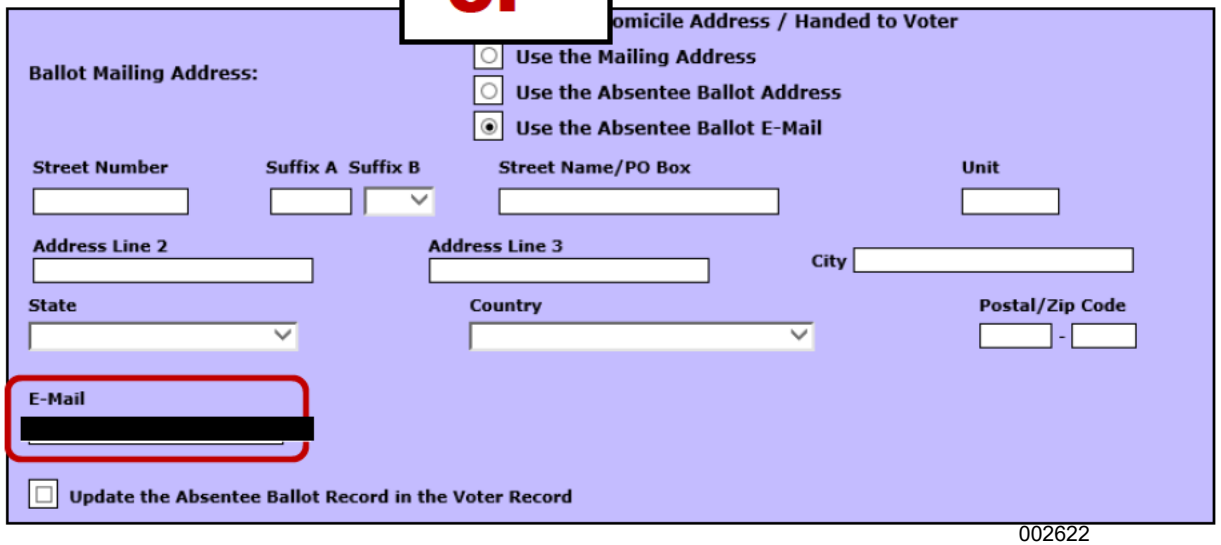


You will be sent the **UOCAVA Absentee Ballots** Via Email

Once Ballots are sent, **start immediately** sending them to your **UOCAVA** Voters

or

Email?



002622

Chapter Review

Can a person request an Absentee Ballot and not be Registered?

Yes they will be sent an Absentee Ballot Not Registered to Vote Package
Help>Instructions

How would you know what Ballot to send to a UOCAVA Voter? Full or Federal Office Only (FOO)?

By how they answered the first question on the FPCA Form
Full Ballot one of the1st, 3 lines, FOO Ballot one of the last 2 lines

What could the voter show to Verify their Absentee Ballot upon returning it in person to the town office?

Voter voluntarily shows appropriate Photo ID
OR
Voluntarily signs a Challenged Voter Affidavit- with a Photo taken or signed Religious Affidavit

Can you start mail/emailing UOCAVA Ballots prior to the 45 Day Dead Line?

YES most definitely, with out delay immediately upon receiving ballots time is of the essence

002623

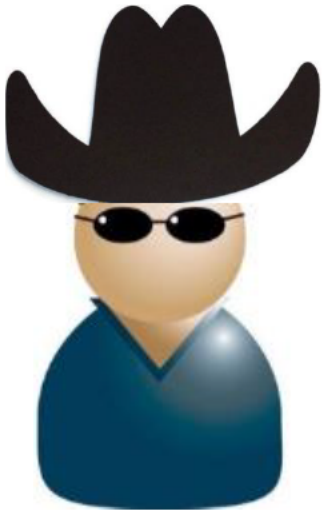
WORK ZONE

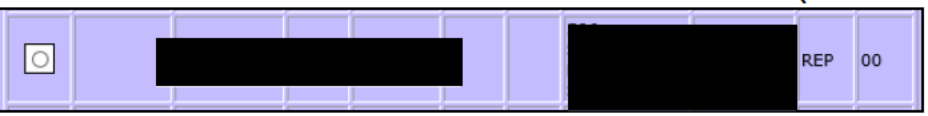
DUPLICATE VOTER - What are They?

They are one and the same but they may have slight differences

Duplicate Voters are created by:

- Not searching in Inquiries first
- Doing **too Narrow** of a search
  EX: (to exact)
- Doing **too Broad** of a search
  EX: (too many names)





Duplicate Voters need to be **MERGED**

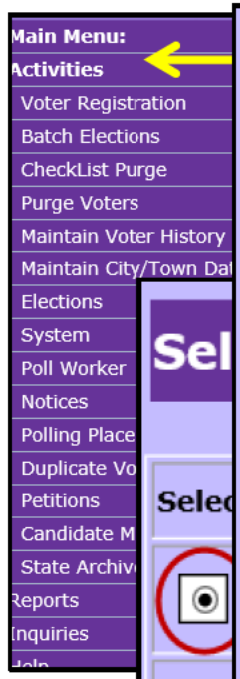
- Searching but missing the voter
- And sometimes there is just not enough information to recognize the voter as already in the system

The Duplicate Voters maybe in your city/town or One in your city/town the Other(s) in another city/town

002624

DUPLICATE VOTER OVERVIEW

WORK ZONE

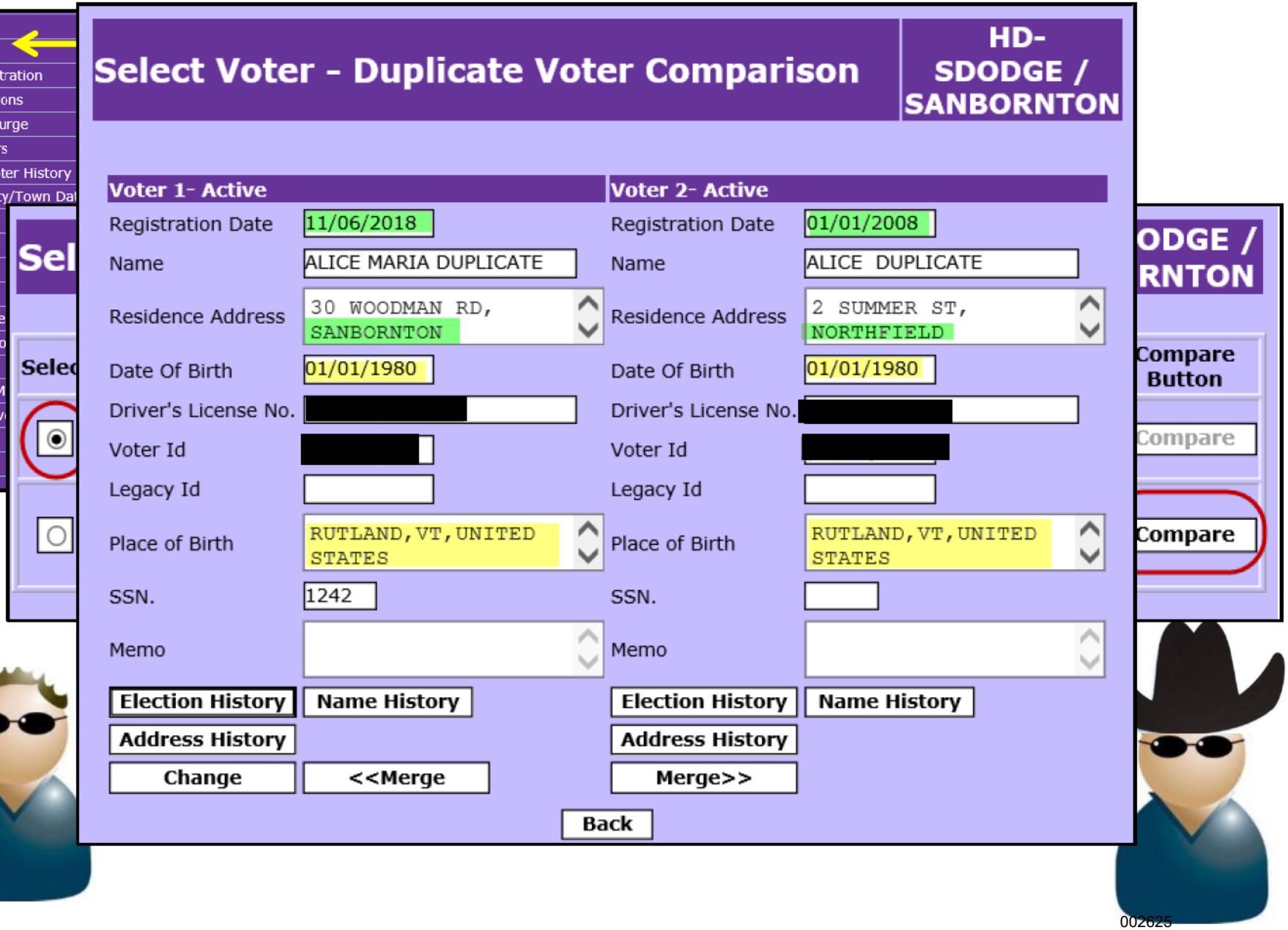


Select Voter - Duplicate Voter Comparison

HD- SDODGE / SANBORNTON

Voter 1- Active		Voter 2- Active	
Registration Date	11/06/2018	Registration Date	01/01/2008
Name	ALICE MARIA DUPLICATE	Name	ALICE DUPLICATE
Residence Address	30 WOODMAN RD, SANBORNTON	Residence Address	2 SUMMER ST, NORTHFIELD
Date Of Birth	01/01/1980	Date Of Birth	01/01/1980
Driver's License No.	[redacted]	Driver's License No.	[redacted]
Voter Id	[redacted]	Voter Id	[redacted]
Legacy Id		Legacy Id	
Place of Birth	RUTLAND,VT,UNITED STATES	Place of Birth	RUTLAND,VT,UNITED STATES
SSN.	1242	SSN.	
Memo		Memo	
Election History	Name History	Election History	Name History
Address History		Address History	
Change	<<Merge	Merge>>	

Back



002625

Introduction 2019

WORK ZONE

DUPLICATE VOTER OVERVIEW-COMPARISON

Select Voter - Duplicate Voter Comparison

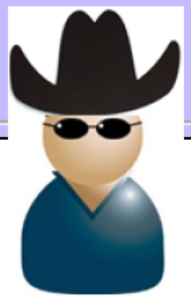
Voter 1- Active		Voter 2- Removed	
Registration Date	03/25/2016	Registration Date	03/09/2004
Name	[redacted]	Name	[redacted]
Residence Address	[redacted] Anytown	Residence Address	[redacted] Othertown
Date Of Birth	[redacted]	Date Of Birth	[redacted]
Driver's License No	[redacted]	Driver's License No.	[redacted]
Voter Id		Voter Id	
Legacy Id		Legacy Id	
Place of Birth	CLAREMONT,NH,UNITED STATES	Place of Birth	CLAREMONT,NH,United States
SSN.		SSN.	
Memo		Memo	
Election History	Name History	Election History	Name History
Address History		Address History	
Change	<<Merge	Merge>>	

Back

If you determine the voters are the same and the voter belongs to you, you must bring the out- of- town voter to your town through: **Add/Change Voter**

When you bring them in the **first** and **last** name must be exactly the same, you may need to make adjustments

The voter will be moved to the address of your duplicate.



DUPLICATE VOTER OVERVIEW-ADD/CHANGE VOTER

WORK ZONE

Registration Card - Add Existing Voter

Mailing Address | Place Of Birth | ...gistered to Vote
Previous Voter Name | Other Information | ...rmation

Name must match so voters will show on the Duplicate Voter Screen

Voter Information: Top

Registration Date: 01 - 01 - 2019 Voter ID: 027003611

Last Name [redacted] First Name [redacted] Middle Name [redacted] Suffix

Date Of Birth - - Age /62years NH Driver's License Number Last 4 Digits of SSN Validate SSN

Confidential Voter ☐

Voter is moved to correct address of your voter

Residence Address: Top

Search Street Name [redacted] Search ☑ Ward Change

Street Number 26 Suffix A Suffix B Street Name [redacted] Unit

Address Line 2 Address Line 3 Residing City/Town State NH

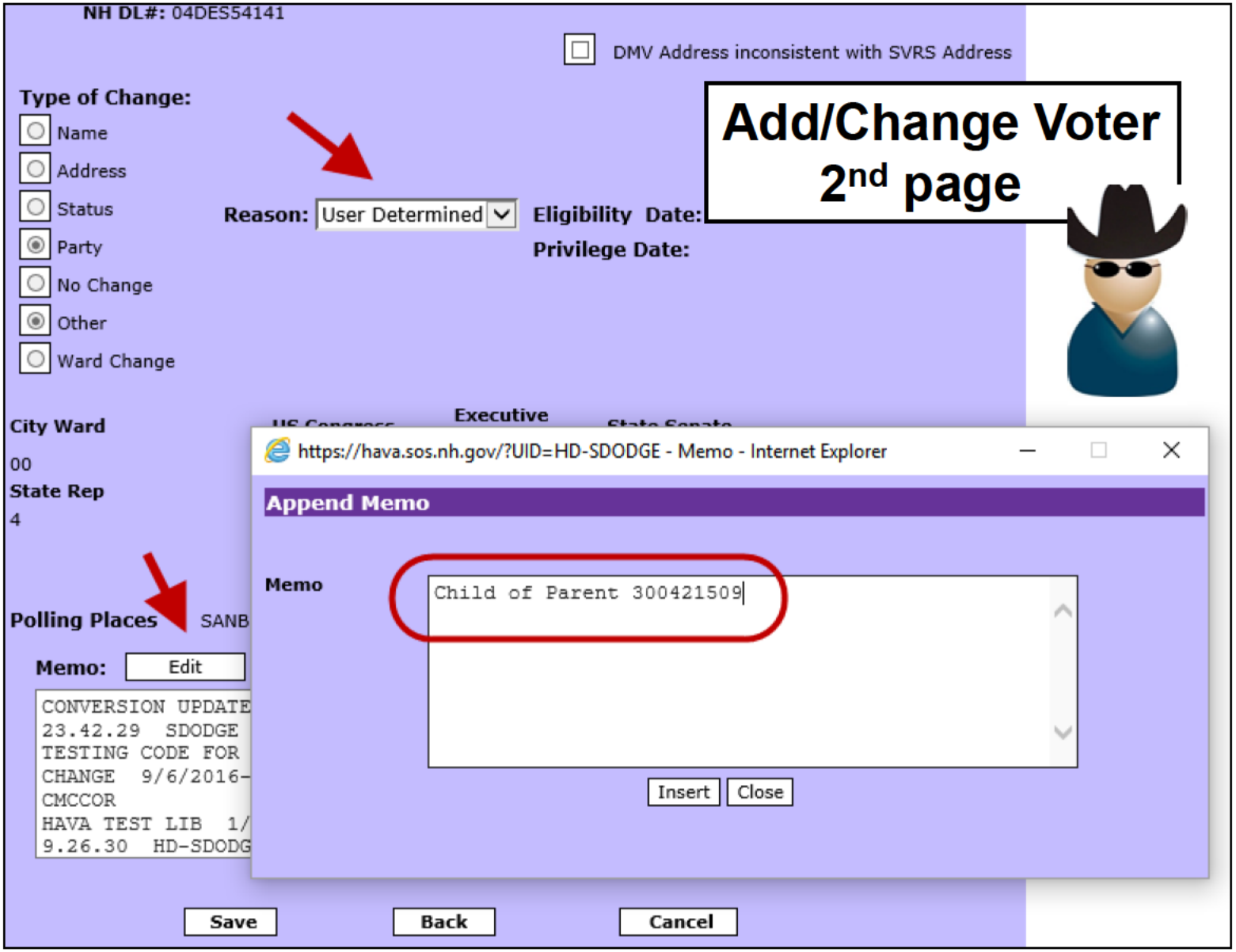
Postal City/Town Postal State Postal/Zip Code 03269 Search Geo Code Longitude -71.488616533 6 Geo Code Latitude 43.1103799285

002627

Domicile Affidavit on File ☐

DUPLICATE VOTER OVERVIEW-ADD/CHANGE VOTER

WORK ZONE



002628

DUPLICATE VOTER OVERVIEW-ADD/CHANGE VOTER

WORK ZONE

DMV Address inconsistent with SVRS Address

Type of Change:

- ○ Name
- ○ Address
- ◉ Status
- ○ Party
- ○ No Change
- ◉ Other
- ○ Ward Change

Reason: Duplicate Voter Record **Eligibility Date:** 02/19/2019

City Ward	US Congress	Executive Council	State Senate	
00	1	1	2	
State Rep	**State Rep Fl**	**County**	**School District**	**Village District**
4		BELKNAP	059	

Polling Places SANBORNTON OLD TOWN HALL

Memo: Edit

CHILD OF PARENT 300421509
2/19/2019-14.21.50 HD-SDODGE

◉ **Do Not Print Correspondence**

○ **Print to Correspondence Batch in System Reminders**

Save **Back** **Cancel**

The Voter being Merged Must be in the **Removed Status**

Go back into **Add/Change Voter**

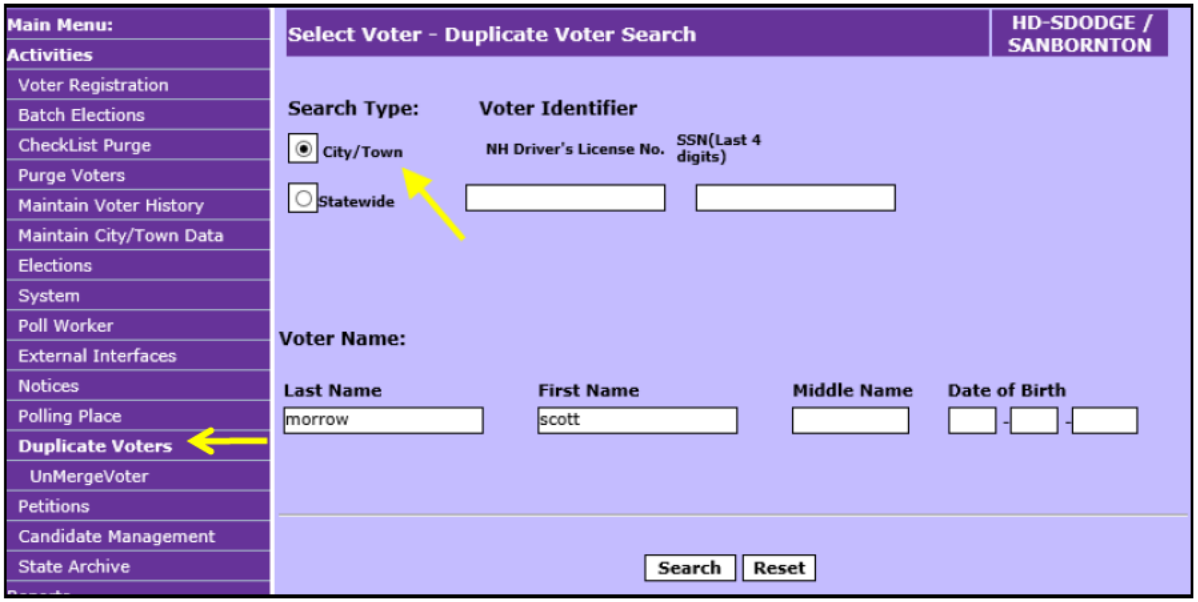
Go to **Other Information** Choose **REMOVED**

Choose **Duplicate Voter** from drop down

002629

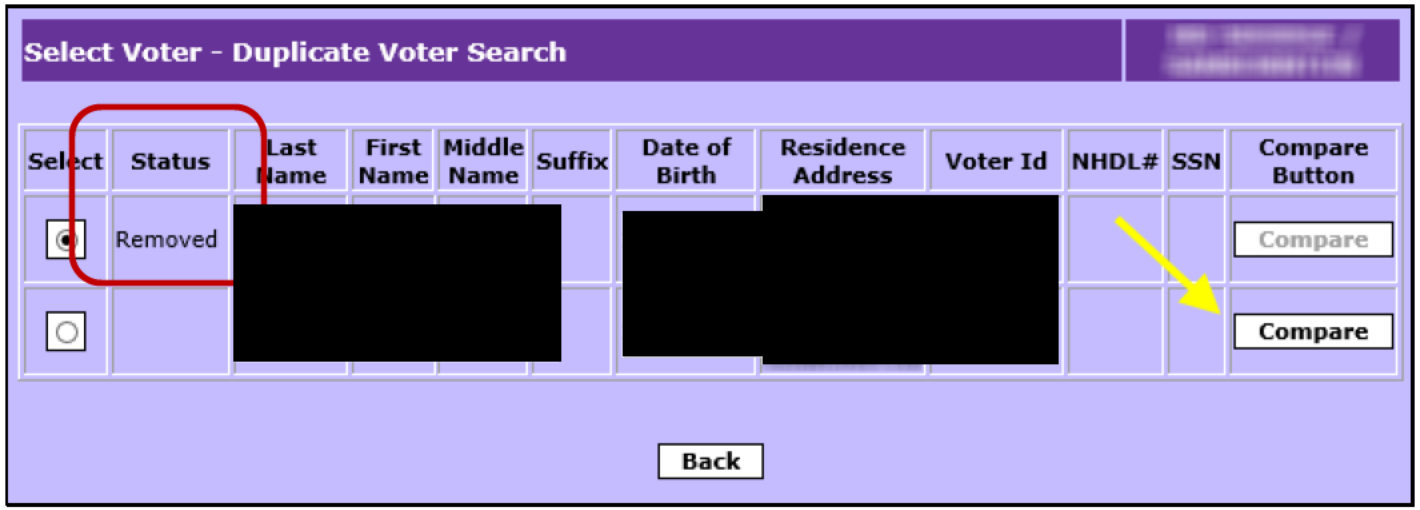
DUPLICATE VOTER

WORK ZONE



Do **Search Type: City/Town**

Compare your two voters



DUPLICATE VOTER

WORK ZONE

Main Menu:

- **Activities**
  - Voter Registration
  - Batch Elections
  - CheckList Purge
  - Purge Voters
  - Maintain Voter History
  - Maintain City/Town Data
  - Elections
  - System
  - Poll Worker
  - External Interfaces
  - Notices
  - Polling Place
  - **Duplicate Voters**
    - UnMergeVoter
  - Petitions
  - Candidate Management
  - State Archive
- Reports
- Inquiries
- Help
- Logout

ter - Duplicate Voter Comparison

Voter 1- Active		**Voter 2- Removed**	
Registration Date	03/25/2016	Registration Date	02/19/2019
Name	[redacted]	Name	[redacted]
Residence Address	[redacted]	Residence Address	[redacted]
			56
			141
			1
			ONT,NH,United
Memo		Memo	CHILD OF PARENT 300421509
Election History	Name History	Election History	Name History
Address History		Address History	
Change	<<Merge	Merge>>	Change

Back

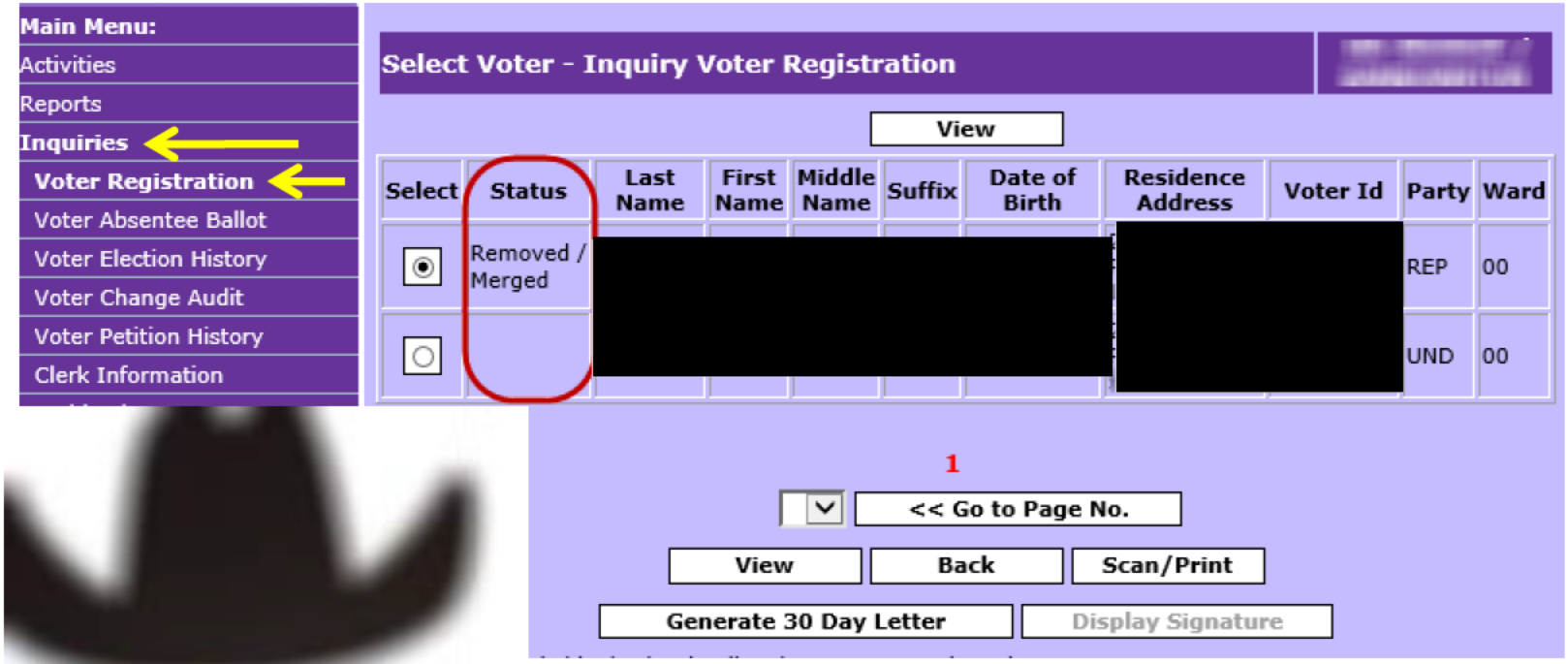
Merge Confirmation

[redacted] erged into [redacted] successfully.

Pop up - You were successful

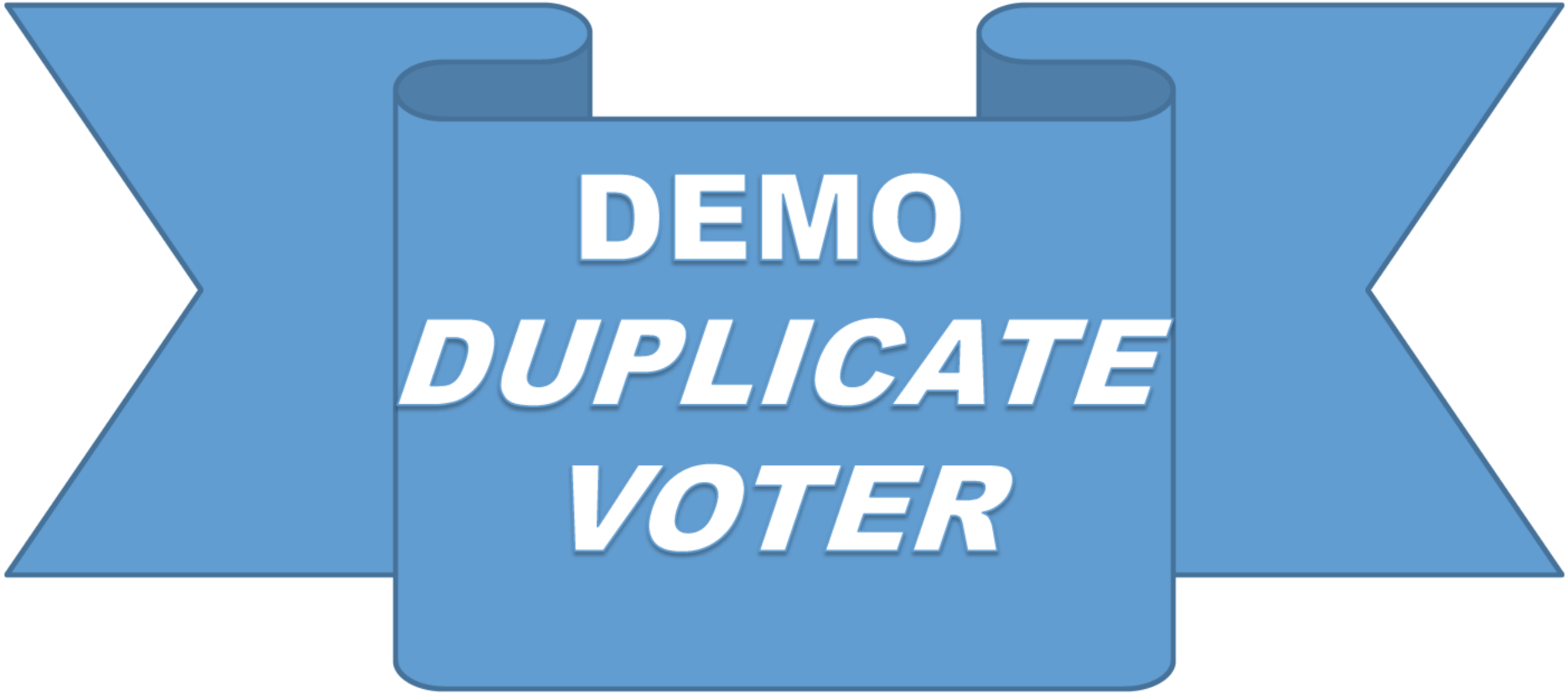
WORK ZONE

INQUIRIES>VOTER REGISTRATION



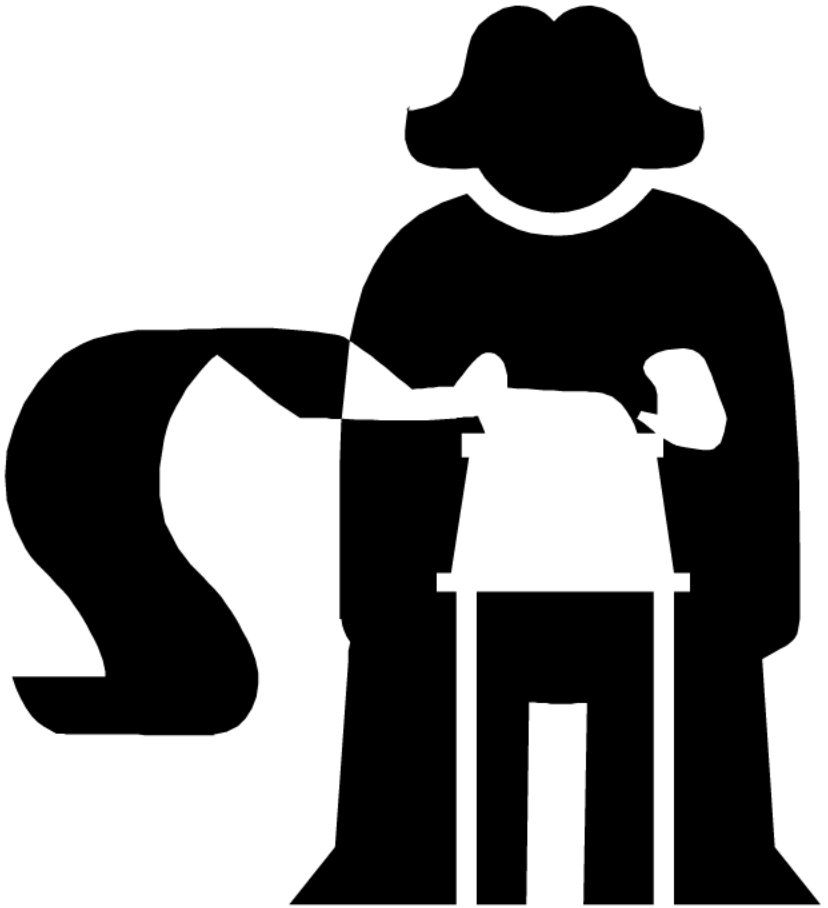
The child record will be in the background as Removed/Merged

002632


DEMO
DUPLICATE
VOTER

Introduction to ElectioNet

Elections & Reports



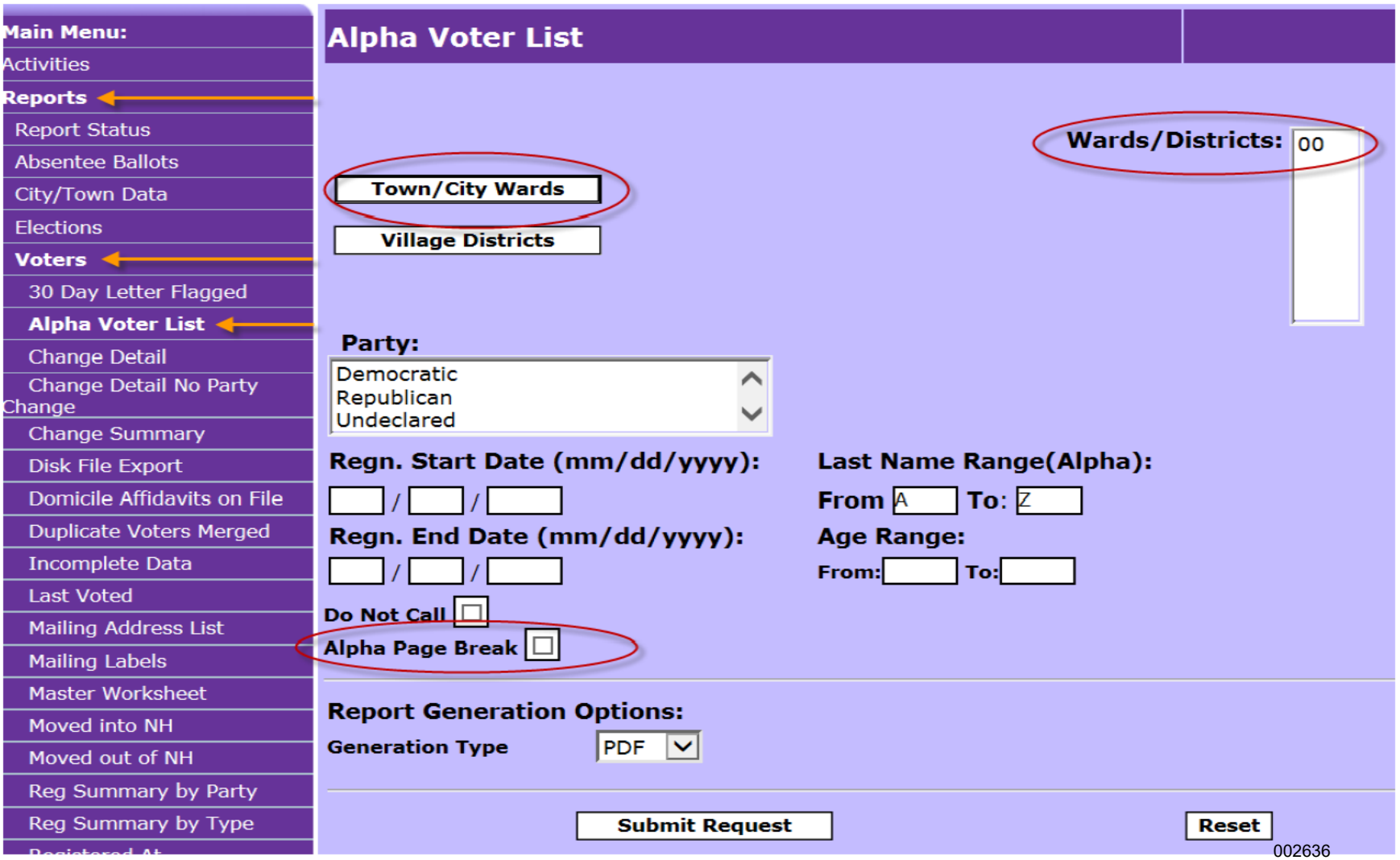
Alpha Voter List - Post & many uses
Change Detail - who did what work
or meeting minutes
Checklist – for Elections
EHAV – Election History Active Voter
Undeclared Re-registration – Return to Und Dom & Qualified Voter
Challenged Voter Affidavit
Out of State Driver's License
Street List – Verify with E911
BarCodes – Scan Election & OOS DL

Elections & Reports

Reports :

- **Alpha Voter**
  - How many voters are on my checklist?
  - What voter records have a default DOB?
  - Do I have any voters that are under 18 years?
- Can be used as a **"Posting"** checklist
- Help / Instructions / **Certification Page Temp** must be attached if posted
- Review for data abnormalities (names, unnecessary mailing address, etc.)

Alpha Voter List



002636

Alpha Voter List – Certification Page

Must be attached to the Posted Alpha Voter List

Date: ___/___/_____ Town/City of _____, NH Ward: _____

Alpha Voter List – Names on Checklist

Certification Page

Total Voters in Town/City: _____

Total Voters by Party: REP = _____ UND = _____ DEM = _____ LIB=_____

Total Voters who have [illegible] still on the reminder

Grand Total: _____

WE, THE SUPERVISO
NH, Ward _____, DO
THE WITHIN LIST CO
ARE, BY ACTUAL DO

Help/Instructions

Supervisors of the Checklist / Board of Registrars

Signature: Print Name:

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

STATE OF NEW HAMPSHIRE

_____COUNTY, NH.

RSA: 654:29

002637

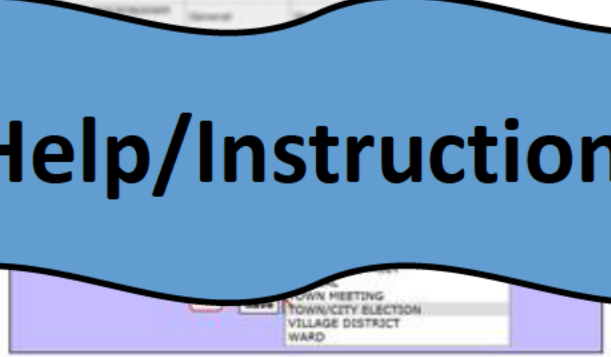
002638

Create a Local Election

How to Create a Local Election

1. Activities / Elections / Maintain Elections
   a. Click "Add New"

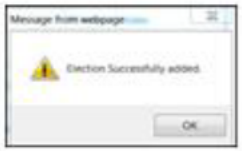
2. Enter "Election Date"
3. Enter "Election Name" Election name MUST contain the name of y "Town/City" (See Ex Below)
4. Select "Election Type" General
5. Select "Election Category" – Town/City Election



6. Leave default to "Non-Partisan"

7. Click "Save"

8. Election has been saved when you receive the Pop up:
   a. "Election successfully added."



9. Election will now appear on the "Maintain Elections" screen.

Help/Instructions

Local Elections must be put in by the **Town/City Clerk**

All State and Federal Elections are entered by the State

The **name of your Town or City MUST** be in the Election Name
Example:
Bow Town and School Election

When choosing a category you must choose City/Town Election for Information to appear in the Voter Look up p App

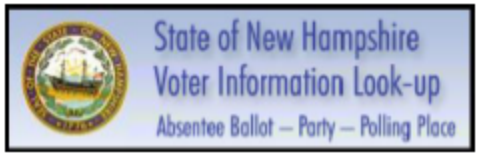
TRACK YOUR BALLOT

Voters: check your party, find your polling place, and more…

Absentee Voters

Track your ballots on:

https://app.sos.nh.gov



Elections & Reports

Reports :

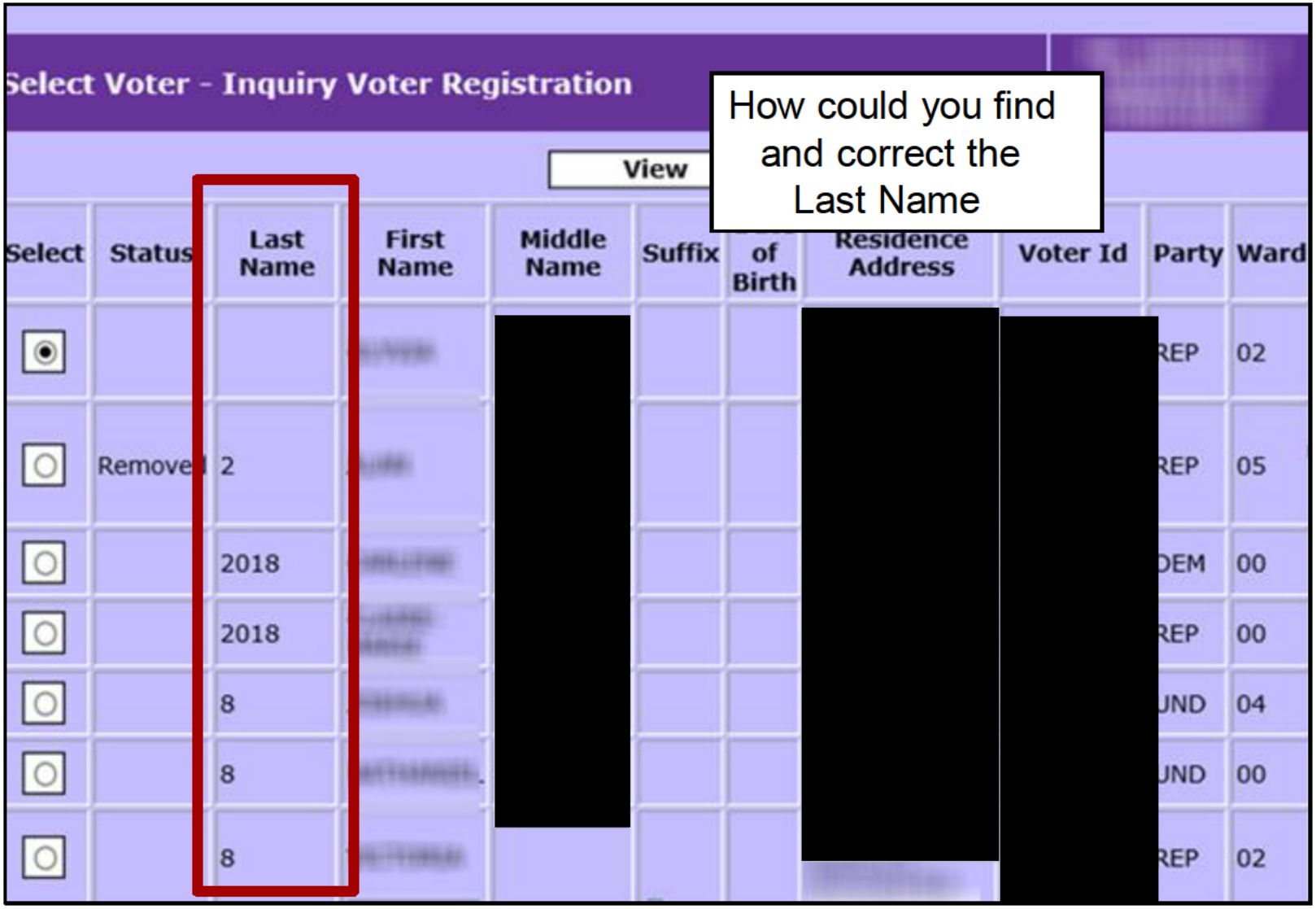
☑ Checklist

- **Official checklist** used at the polls
- Other uses - posting, selling, election day registration scanning
- **Help -> Instructions -> How to Generate**

- RSA 654:45 III – "The voter database shall…be the official record of eligible voters for the conduct of all elections held in this state."

  Will give Barcodes for Election Day Registrations

What's on your Checklist ?



002642

What's on your Checklist ?

Review your Checklist for Anomalies

☐ DEM [redacted] ☐ [redacted] 00 [redacted]
NH 03840
- 0

☐ DEM [redacted] ☐ [redacted] 00
AVE NH 03840,
UNITED STATES

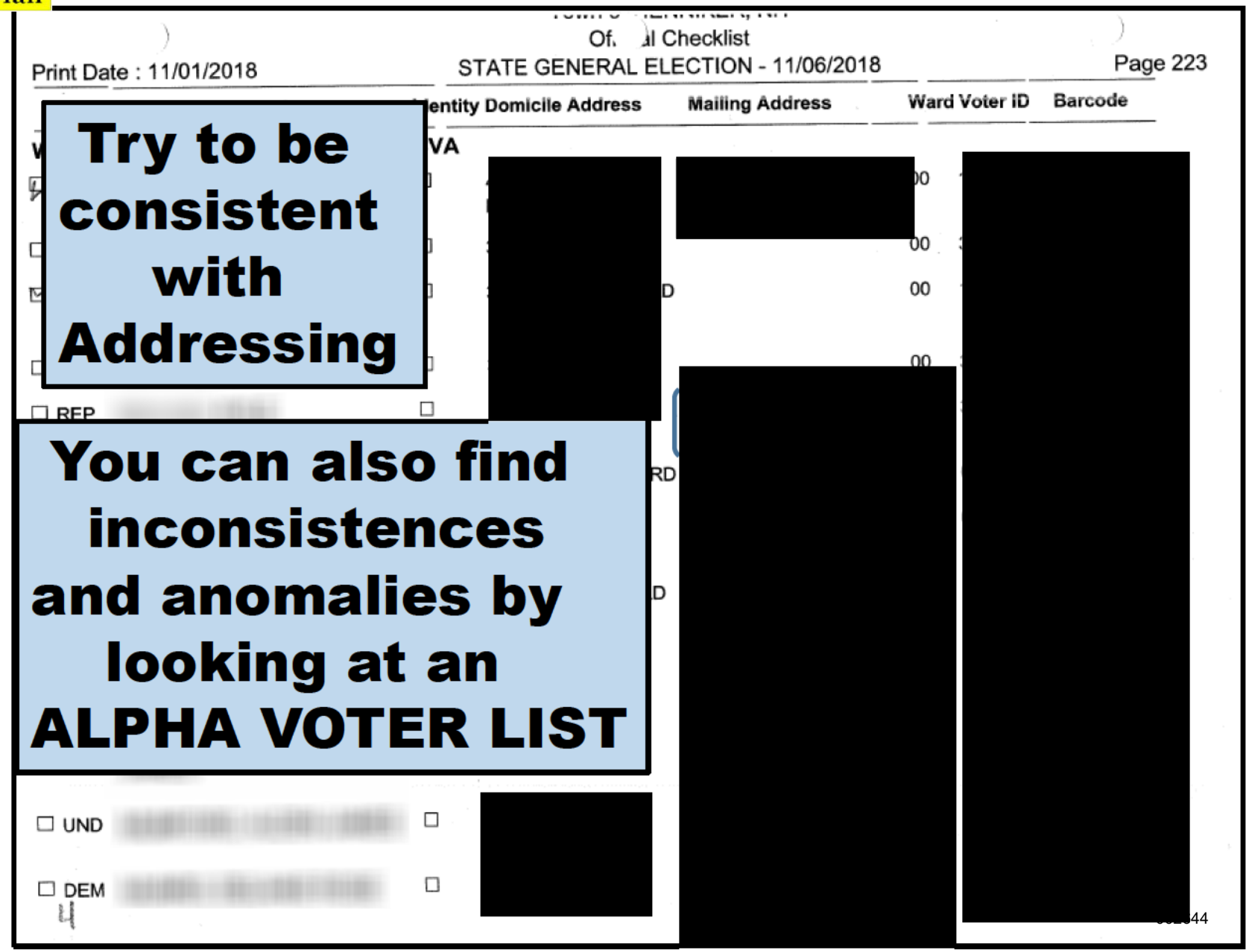
Print Date : 03/05/2016 TOWN OF [redacted] ELECTION - 03/08/2016 Page 1

Voter Name	Identity Domicile Address	Mailing Address	Ward Voter ID	Barcode
Ward 00	**CVA**			
☐ [redacted]	☐ [redacted]		00	[redacted]

☐ DEM [redacted] ☐ 1 OVERSEAS CITIZEN FEDERAL BALLOT ONLY [redacted] 00

002643

What's on your Checklist ?



Elections & Reports

Insert Blank Page w/Lines for Checklist Election Day Registrations
Can be found in: Help->Instructions->Checklist – New Voter Template

Town of SANBORNTON, NH
Official Checklist

Print Date : 09/27/2017 TEST GENERAL ELECTION - 11/07/2017 Page 6

Party Voter Nam ode

Ward 00 CONT.

Letter B New Registered Voter List Page No. 6-A

Party	Last Name	First Name	Middle Name	CVA	Address
✓REP	~~Baker,~~	[redacted]		MA	[redacted]
✓ LIB	~~Backster~~			✓	
✓DEM	~~Brandon~~				
UND	~~Blackburn~~				

Sample of a marked checklist for a General Election

Page 1

Party	Voter Name	Identity Domicile Address	Mailing Address	Ward	Voter ID	Barcode
Ward 00		CVA				
☑ LIB	[redacted]	☑ [redacted]	PO Box 95 ~~PO BOX 123,,~~	00	300348386	
☐ DEM		☐				
A.V. ☑ REP		☐				
☑ UND		☐ MA				
☑ UND		☑				

On Election Day, Supervisors are the only Election Officials that may strike a name from the Checklist:
(using information supplied by the Show Reminder Screen)

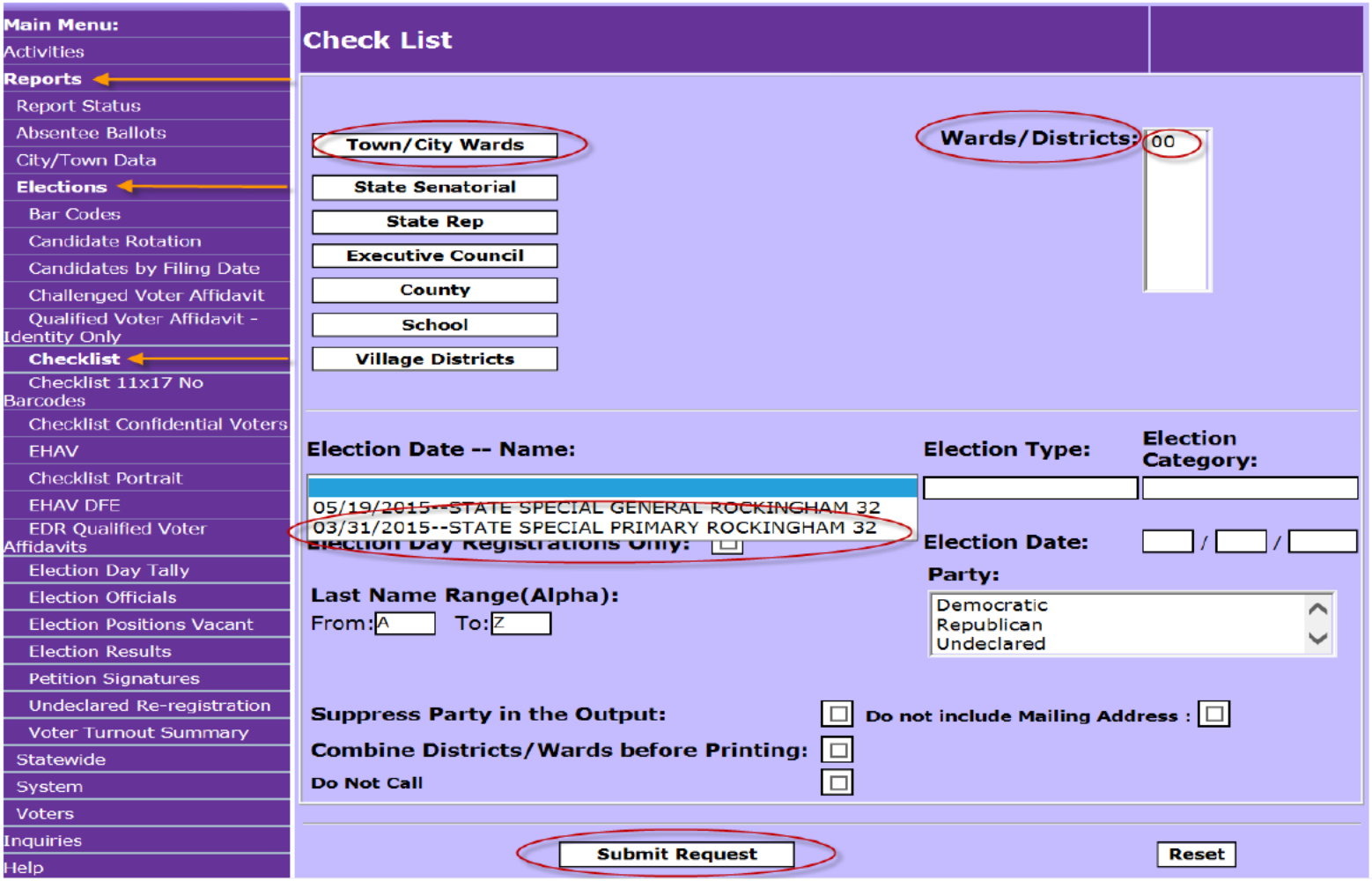
Sample of a marked checklist for a Primary Election

Party	Voter Name	Identity Domicile Address	Mailing Address	Ward	Voter ID	Barcode
Ward 00		CVA				
☑ UND	[redacted]	☑ [redacted]				
☐ DEM		☐				
☐ REP		☐				
☑ UND		☐ MA				
☑ UND		☑				

002646

Elections & Reports

How to Run a Checklist



002647


DEMO
Check List

AFTER ELECTIONS REPORTS

Before the Election Reports

Alpha Voter List: This is the recommended posted checklist, can be used as a Check-In for meetings

Checklist: Must be used at all elections by ballot clerks to check-in the voters, run a checklist for the election day registrations to produce a bar code to Batch Election

Return to Undeclared for Primary: Run for Primary Only, list of voters registered as Undeclared

Street Voter List or Street List: Look at registered voters on a Street or a list of Streets with ranges

After Election Reports

Activities>Reports>Elections

Barcodes and Barcodes for States: For scanning checklist in Batch Elections and Batching Out of State DL's

Checklist: Will give you the Barcode for Election Day Registration Voters (If entered correctly)

Challenged Voter Affidavits: Lists Election Day Registrations scanned as having signed a CVA

Qualified Voter Affidavits-Identity Only: Lists Election Day Registrations who signed the QVA for Identity or only gave the last 4 digits of their SS#

OOS DL Presented to Ballot Clerk: Lists Voters scanned who showed the Ballot Clerk an Out of State Driver's License

EHAV: Lists voters that where scanned for election participation also may be run after scanning each letter of the alphabet from the Marked Checklist to verify number and name of voters scanned

EHAV DFE: Lists voters that were scanned for election participation in a disc file report

Activities>Reports>Voters

Domicile Affidavits on File: Lists voters that registered and signed a Domicile Affidavit

Alpha Voter List: List the voters by registration day date, may be used to get an Election Day Registration voter's ID # to type in Batch Election if the voter was entered in incorrectly.

Change Detail: Will give you details on any additions/changes, etc. and the person who entered or touched the voter record.

2019 v2

Quick Reference

002649

Elections & Reports

Main Menu:
- Activities
- Voter Registration
- Batch Elections
- Multiple Election History
- Return to Undeclared
- Record Out-of-State Driver's License State
- CheckList Purge
- Purge Voters
- Maintain Voter History
- Maintain City/Town Data
- Elections
- System
- Poll Worker
- External Interfaces
- Notices
- Polling Place
- Duplicate Voters
- Petitions
- Candidate Management
- State Archive
- Reports
- Inquiries

Record Out-of-State Driver's License State

HD-SDODGE / SARGENT'S PURCHASE

Election Date & Name

03/15/2018--ELECTIONET TEST PRIMARY

☐ Check this box and click save If:
no Out-of-State driver's license were recorded for this election

Voter ID's	Out-of-State Driver's License State

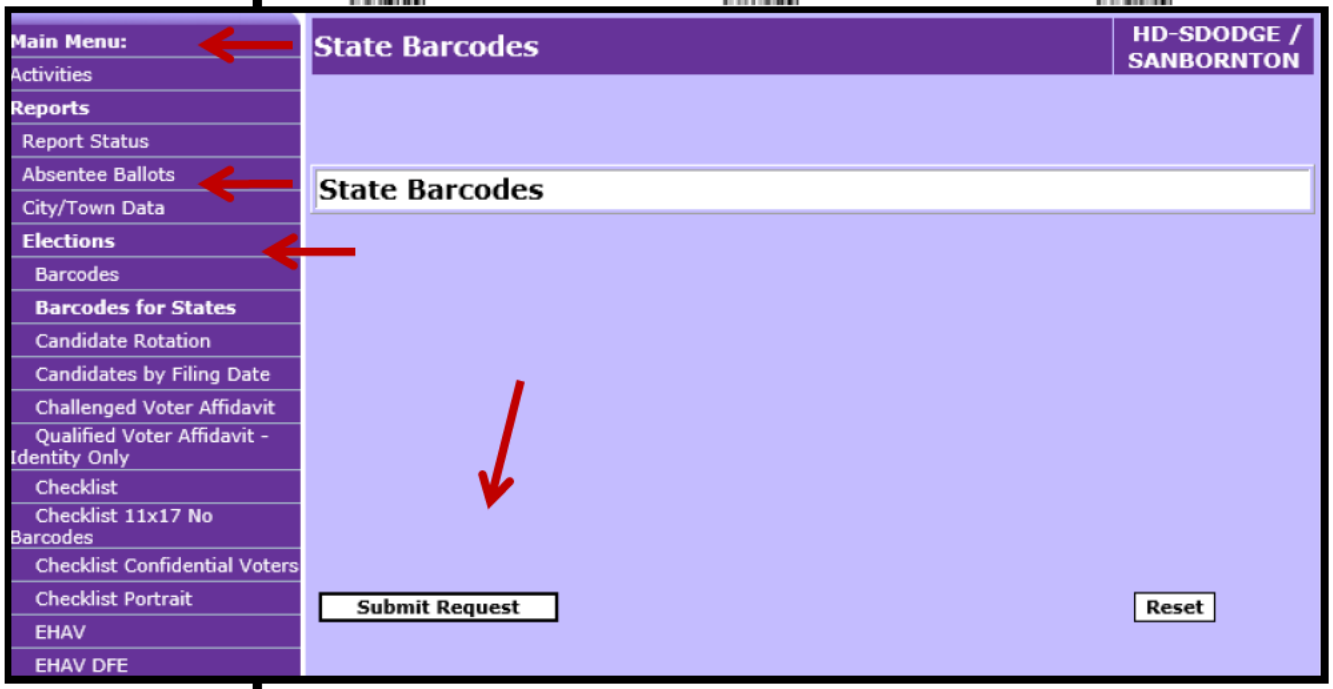
*** New Feature ***

No More
Tally and Summary Reports

Save Reset

002650

Alabama - AL
Alaska - AK
American Samoa - AS
Arizona - AZ
Arkansas - AR
California - CA
Colorado - CO
Connecticut - CT
Delaware - DE
District of Columbia - DC
Florida - FL
Georgia - GA

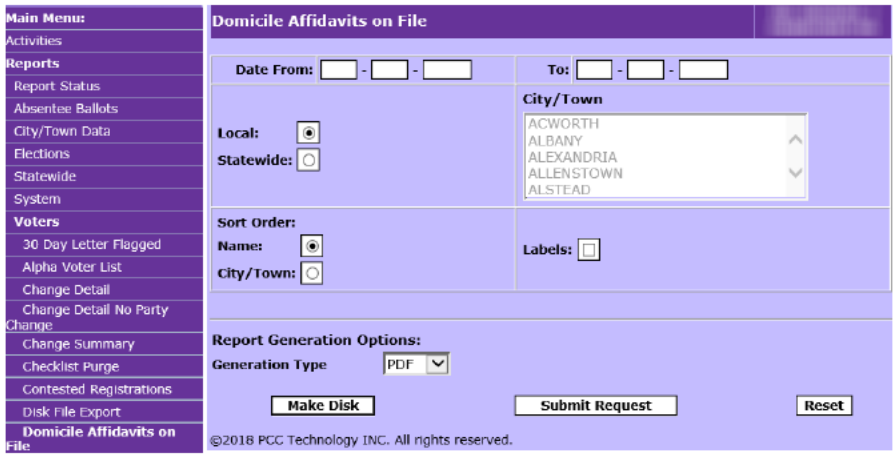


Rhode Island - RI
South Carolina - SC
South Dakota - SD
Tennessee - TN
Texas - TX
US Virgin Islands - VI
Utah - UT
Vermont - VT
Virginia - VA
Washington - WA
West Virginia - WV
Wisconsin - WI
Wyoming - WY

OOS DL State Bar Code

DOM REPORT

Reports>Voters>Domiciled Affidavit



01/18/2019 — Domicile Affidavit on File — Page 1

From: 01/01/2016 To: 12/31/2017

Generated By : HD-SDODGE

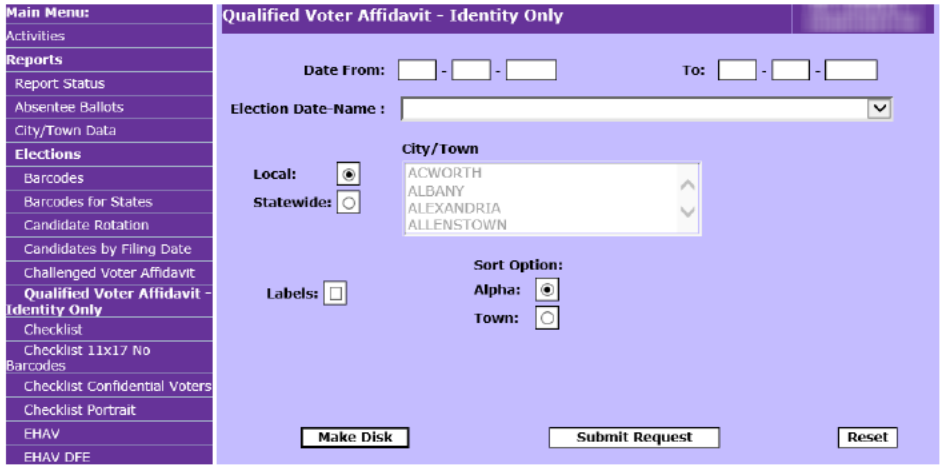
Voter ID	Name	Domicile Address	Mailing Address
SANBORNTON -- 00			
[redacted]	[redacted]	100 [redacted] SANBORNTON, NH, 03269	
[redacted]	[redacted]	100 [redacted] SANBORNTON, NH, 03269	
[redacted]	[redacted]	184 [redacted] SANBORNTON, NH, 03269	
[redacted]	[redacted]	274 [redacted] SANBORNTON, NH, 03269	
[redacted]	[redacted]	76 [redacted], SANBORNTON, NH, 03269	

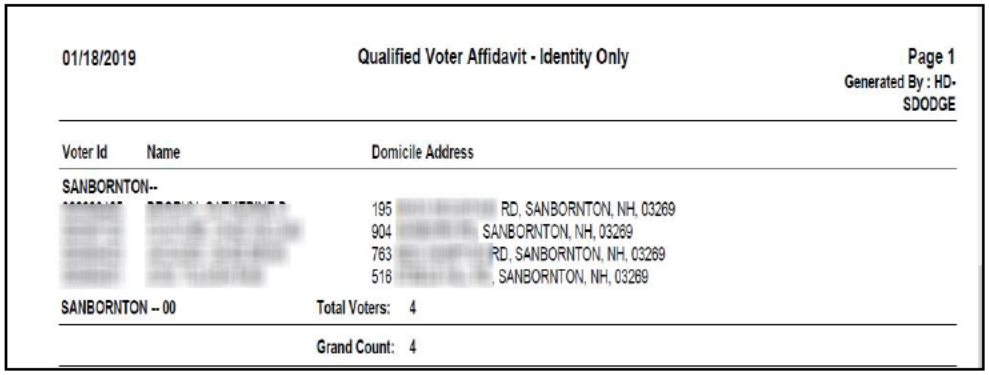
SANBORNTON -- 00 Total Voters: 5

Grand Count: 5

QVA REPORT

Reports>Elections>Qualified Voter Affidavit





01/18/2019 — Qualified Voter Affidavit - Identity Only — Page 1

Generated By : HD-SDODGE

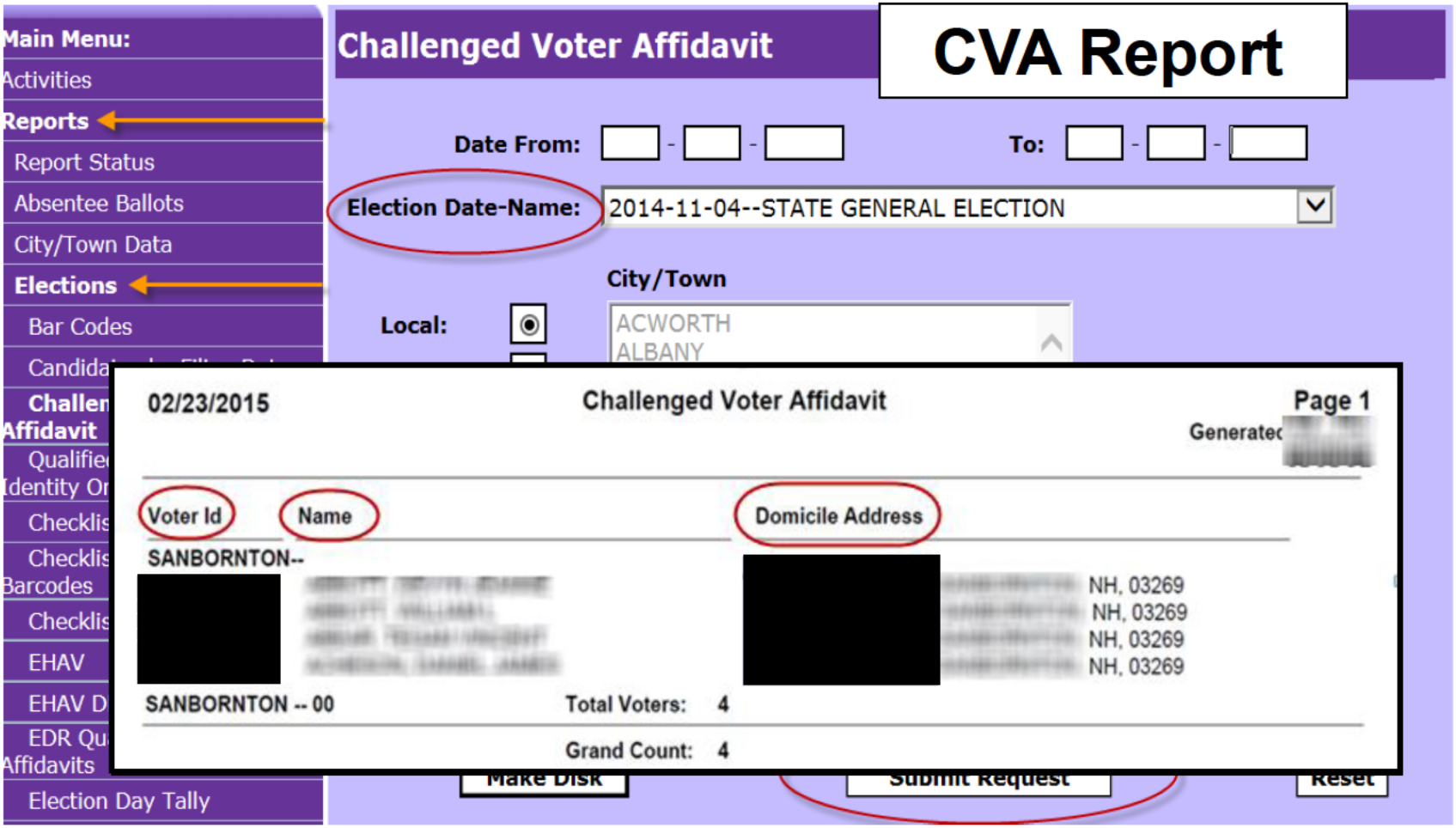
Voter Id	Name	Domicile Address
SANBORNTON--		
[redacted]	[redacted]	195 [redacted] RD, SANBORNTON, NH, 03269
[redacted]	[redacted]	904 [redacted] SANBORNTON, NH, 03269
[redacted]	[redacted]	763 [redacted] RD, SANBORNTON, NH, 03269
[redacted]	[redacted]	518 [redacted], SANBORNTON, NH, 03269

SANBORNTON -- 00 Total Voters: 4

Grand Count: 4

002652

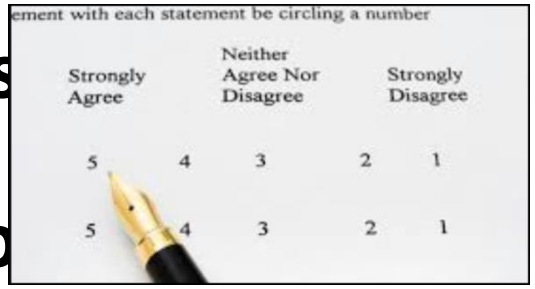
Elections & Reports



Introduction to Electio*Net*

Help / Instructions

Introduction to ElectioNet



- Have you completed your Ques
- Please remember to hand in yo before you leave.
- Thank you for attending.
- Have a safe drive home.

The 1

Team

Introduction to ElectioNet

002656

NASS/NASED Social Media Working Group Conference Call
May 21, 2019

Participants:

Maria Benson, NASS Director of Communications | Amy Cohen, NASED Executive Director

Twitter	Kevin Kane	kkane@twitter.com
Twitter	Bridget Coyne	bridget@twitter.com
Facebook	Eva Guidarini	eguidarini@fb.com
Google	Joe Dooely	jdooley@google.com
Google	Erica Arbetter	arbetter@google.com
Google	Maria Giannopolous	giannopolous@google.com

NASS Members Communications Staff

Washington	Erich Ebel
Washington	Kiran Boyal
Connecticut	Gabe Rosenberg
Connecticut	Stephanie Sponzo
Louisiana	Brandee Patrick
Rhode Island	Nicole Lagace
Rhode Island	Arianna Conte
Indiana	Valerie Warycha
Kansas	Katie Koupal
Arizona	Murphy Hebert
Mississippi	Leah Rupp Smith
Wyoming	Will Dinneen
Vermont	Eric Covey
Colorado	Jenny Flanagan
Colorado	Serena Woods
New Mexico	Alex Curtas
Ohio	Grant Shaffer
Ohio	Jon Keeling

NASED Members Communications Staff

New York	Ryan Richmond
New York	Cheryl Couser
Wisconsin	Reid Magney
Oklahoma	Misha Mohr
North Carolina	Emily Lippolis
Illinois	Matt Dietrich
Maryland	Cortnee Bryant

NASS Communications Director Maria Benson noted that the call was the first meeting of the working group, and noted that working group was created following a communications roundtable with social media platforms at the NASS winter conference. She noted that many of the roundtable participants expressed an interest in establishing a mechanism for regular dialogue between communications staff and social media organizations in order to share information and discuss relevant issues and concerns.

Representatives from Facebook, Google, and Twitter provided a brief overview of what they hope to accomplish through participation in the working group. Each organization emphasized that they want to help provide useful, accurate election information to users of the respective platforms. In addition, Facebook noted that they are currently focusing on deciding which products to launch for the 2020 election and evaluating lessons learned from recent elections in India and the EU that can be applied in the U.S. Twitter noted that they released a midterm review report in January that discussed findings from the 2018 election along with recent product changes and policy improvements. They added that they are working on adding candidate labels (e.g. office running for, jurisdiction) and emojis next to hashtags that encourage people to share that they participated in an election. Google (along with Facebook and Twitter) noted that they want to continue to build collaborative relationships with election officials to ensure the accuracy of tools and services for voters.

Communications staff from the states represented on the call provided a brief overview of what they hope to accomplish through participation in the working group. Many of the participants noted similar goals, including sharing best practices and learning from other states and the social media platforms on ways to deal with misinformation heading into the 2020 election; providing social media platforms with direct feedback on the types of issues elections officials are seeing on social media; learning new strategies for utilizing social media to provide election information; helping voters navigate social media to find accurate sources of information; sharing information gained through the working group with counties and local jurisdictions; learning ways to deal with groups that are legitimate and well-intentioned but providing election information on social media that is confusing or inaccurate; learning ways to deal with inaccurate news articles that get shared and distributed on social media.

Facebook and Twitter were asked to provide an overview of their account verification process. Twitter noted that they have a one-on-one verification process that requires a government email address. They added that they provide assistance that includes walking through creating the profile and said states can reach out to gov@twitter.com to start that process.

Facebook noted that states (as well as county/local offices) can send an email to Eva Guidarini (eguidarini@fb.com) to start the verification process, or reach out to their Facebook regional team. They noted that states will need to provide a link to the page they want to get verified. Ms. Benson and Ms. Cohen noted that they have contact information for the Facebook regional teams that they can provide to the working group. Ms. Benson asked that states CC her as well in case any question or issues come up that NASS can provide assistance with. Ms. Cohen asked the same of her members.

In response to questions from several participants, the social media platforms provided additional information about the verification process. Facebook noted that that verification process also applies to Instagram (same points of contact for both). They added that the verification criteria are slightly different for Facebook and Instagram, but noted that they haven't had issues with verification for a government account.

Google noted that they have a pilot program for a YouTube verification process and said states can reach out to government@youtube.com or civic-outreach@google.com for information on that process.

Facebook noted that there are two levels of verification: a gray badge, primarily for small business, and a blue badge that indicates who the profile is and why it's notable. They said the blue badge is automatically the verification process for states. They noted that if states see a blue check mark next to their profile name in the search results that means it has already been verified.

Twitter noted that there should not be any issues getting both a Secretary of State individual account and a Secretary of State office account verified. They recommended states utilizing both accounts since users sometimes have different preference for interaction. They noted that states can reach out to gov@twitter.com for assistance in designing ways to utilize the different accounts.

Facebook noted that the blue verification badge/checkmark authorization process is separate from the verification process for election ads. They noted that the verification for both processes can take time and noted they can provide assistance to states and local jurisdictions with those processes.

Facebook noted that their policies prohibit impersonating another account. They noted that verification helps combat impersonation by indicating the official account, but said an imposter account will be taken down whether or not the person being impersonated has been verified, or is even on Facebook. Twitter noted that they have robust impersonation policies. They noted that the blue checkmark for verified accounts allows bystanders to report instances of impersonation.

Twitter and Facebook were asked by Ms. Benson if a Secretary of State that is not on one or both platforms could create an account as a placeholder and have it verified even if they don't utilize the platform. Twitter noted that if a candidate is running for office, they can provide assistance reserving handles for unique cases. Facebook noted that a page needs at least one initial post for verification and added that the page could also be unpublished.

The social medial platforms discussed some of the issues and concerns mentioned by states. One of the platforms noted that several states mentioned it would be beneficial to have best practices, and the platform asked for clarification on what type of best practices states were referring to. A state indicated that it would be useful to have best practice information on how to respond when false information is spread on social media. Twitter noted that NASS and NASED participated in a partner support portal in 2018 and said they are looking to expand that to individual state offices. They added that in April they announced a feature not yet rolled out in America, that anyone can report voter suppression activity in app, which would include misinformation about how to register, requirements for voting, misleading statements about the election date/time, etc.

One of the participants noted that they reached out to the platforms during the last election regarding false reports on social media about people being removed from the registration rolls but never heard back. They asked how the platforms plan to respond to and combat misinformation in 2020. Facebook noted that they added a reporting feature to allow any user to report misinformation and said they will also have a reporting channel for election officials. They noted that they send the misinformation reports to fact checkers who can look into the content and mark the information as false if it is inaccurate. Twitter noted that they launched the voter suppression reporting tool in April and don't have any data yet on that

process, but said they removed nearly 6,000 Tweets identified as attempted voter suppression during the 2018 election.

Ms. Benson noted that some states have expressed concerns about labeling activity as voter suppression for reporting purposes since the definition may vary among different groups. She asked if any of the platforms had discussed relabeling that reporting process. Facebook noted that they understand the concerns from some states and based on that feedback they are currently in the process of changing the name of the reporting process to the Voter Integrity Policy. They noted that only the name is changing and said the actual reporting process will be the same.

Ms. Cohen asked what constitutes impersonation for purposes of the platforms policies on imposters. Twitter indicated that their policy is straightforward and said they will suspend the account of anyone posing as another person, brand or organization in a deceptive manner. Facebook noted that their policies on misrepresentation cover imposters and said they have reporting mechanisms for impersonation. They added that in some cases a user has to be pretending to be someone else, not just using their name, to constitute impersonation in order to allow for instances like satire that that don't involve claiming to be the actual person. They noted that these situations also can raise 1st amendment issues. The noted that fact checkers make determinations on impersonation and they have a content review process to ensure the right action is taken. Ms. Cohen expressed concern about voters getting inaccurate from those sites that technically don't violate the impersonation policy but are not the actual person or organization. Facebook noted that the verification method is one method to help people know the official government sources, as well as institutions included in Facebook Town Hall to show the official sources.

Ms. Benson asked how Google ranks election information in search results. Google noted that it depends on a variety of factors and noted that when searching for an elected official a user may get a knowledge panel at the top of the results. They noted that if an elected official has a knowledge panel for their name in the search results they can claim the information and make any edits to ensure the information is accurate. They indicated that it's difficult to get misinformation to come up as a top search result but said if it did happen they would address it as soon as possible.

A participant expressed concern about Facebooks relationship with TurboVote based on issues that occurred during the last election. They indicated that those types of situations lead to distrust of social media and are an example of why social media voter registration drives are problematic. They encouraged Facebook to link directly to state voter registration sites as opposed to using TurboVote. Facebook noted that they will be running some sort of registration product on Facebook going forward but indicated that that no decision has been made yet. They added they are working with a couple states on a pilot project to explore linking directly to states sites and said they will provide more information on that effort in the future.

Facebook noted that they expanded their political ad archives reporting function. Twitter noted that they rolled out an ad transparency center last summer that includes all ads run by candidates. Google noted that they are working to bring their ad transparency tools to the state level for 2020.

Ms. Benson and Ms. Cohen noted that the next call will be held in August and added that initial agenda items include mis/disinformation and advertising policies. They asked participants to reach out to them with any questions.

The call adjourned at 3:10 PM EDT.

Look around your office or home and select 4 to 5 different things or a phrase that could be your password containing 24 – 50 characters. Passwords may include upper and lower case letters, numbers, special characters and spaces.

NOTE: You may <u>NOT</u> use any of the examples below for your password. Think of a picture containing the items or phrase.

[redacted]   

[redacted]  

[redacted]   

[redacted]  

[redacted]  

[redacted]  

[redacted]   

[redacted]   

[redacted]  

002662

Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated January 28, 2019

The Designation of Election Systems as Critical Infrastructure

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. Subsequently, in January 2017 the Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. The designation sparked some initial concerns by state and local election officials about federal encroachment of their prerogatives, but progress has been made in overcoming those concerns and providing assistance to election jurisdictions.

What Led to the Designation?

In August 2016, the Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at exfiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin. That same month, DHS contacted state election officials to offer cybersecurity assistance for their election infrastructure. Most states accepted the offer. Although the cyberattacks did not appear to affect the integrity of the election infrastructure, some observers began calling for it to be designated as critical infrastructure (CI). On January 6, 2017, the Secretary of Homeland Security announced that designation.

What Is Critical Infrastructure?

Under federal law, CI refers to systems and assets for which "incapacity or destruction ... would have a debilitating impact on security, national economic security, national public health or safety, or any combination" of them (42 U.S.C. §5195c(e)). Most CI entities are not government-owned or -operated. Presidential Policy Directive 21(PPD 21) identified 16 CI sectors, with some including subsectors. Sectors vary in scope and in degree of regulation. For example, the financial services sector is highly regulated, whereas the information technology sector is not. Election infrastructure has been designated as a subsector (EIS) of government facilities. That sector includes two previously established subsectors: education facilities, and national monuments and icons.

The Homeland Security Act of 2002 (P.L. 107-296) gave DHS responsibility for several functions aimed at promoting the security and resilience of CI with respect to both physical and cyber-based hazards, either human or natural in origin. Among those functions are providing assessments, guidance, and coordination of federal efforts.

Each CI sector has been assigned one or two federal sector-specific agencies (SSAs), which are responsible for coordinating public/private collaborative efforts to protect the sector, including incident management and technical assistance. DHS has regulatory authority over two sectors: chemical and transportation systems. It serves as SSA for several, including the EIS.

The components of the EIS as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns.

Does the Designation Permit Federal Regulation of Election Infrastructure?

DHS does not have regulatory authority over EIS. Five other agencies have significant roles with respect to federal elections, but none has claimed regulatory authority over the EIS:

- The Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA, P.L. 107-252), provides a broad range of assistance to states, including development of voluntary technical standards for voting systems, voluntary guidance on implementing HAVA requirements, and research on issues in election administration. It also has statutory authority for administering formula payments to states to assist them in meeting HAVA requirements and improving election administration, including $380 million appropriated in FY2018 in response to security concerns.
- The National Institute of Standards and Technology (NIST) assists the EAC on technical matters, including development of the voting system standards, certification of voting systems, and research.
- The Department of Justice (DOJ) has some enforcement responsibilities with respect to requirements in HAVA and other relevant statutes.
- The Department of Defense (DOD) assists military and overseas voters.
- The Federal Election Commission (FEC) is responsible for enforcement of campaign finance law but is not involved in election administration by state and local jurisdictions.

HAVA expressly prohibits the EAC from issuing regulations of relevance to the CI designation, and it leaves the methods of implementation of the act's requirements to the states. However, it does permit DOJ to bring civil actions if necessary to implement HAVA's requirements.

What Does the Designation Mean?

While both DHS and the EAC provided assistance to states in addressing the security concerns that arose in the run-up to the November 2016 election, the CI designation had several notable consequences:

- It raised the priority for DHS to provide security assistance to election jurisdictions that request it and for other executive branch actions, such as economic sanctions that the Department of the Treasury can impose against foreign actors who attack elements of U.S. CI, including tampering with elections.

- It brings the subsector under a 2015 United Nations nonbinding consensus report (A/70/174) stating that nations should not conduct or support cyber-activity that intentionally damages or impairs the operation of CI in providing services to the public. It also states that nations should take steps to protect their own CI from cyberattacks and to assist other nations in protecting their CI and responding to cyberattacks on it. The report was the work of a group of governmental experts from 20 nations, including Russia and the United States.

- It provided DHS the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms are used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors. For example, both the FBI and the Office of the Director of National Intelligence (ODNI) have participated in briefing election officials on threats to the EIS.

Among the coordination mechanisms for the subsector are the following:

- *Government Coordinating Council.* The GCC consists of representatives of DHS, the EAC, state election offices from 13 states, 7 counties, and 1 city, representing 18 states altogether. The GCC facilitates coordination across government entities both within EIS and in other sectors. Activities include communications, planning, issue resolution, and implementation of the security missions of the entities.

- *Sector Coordinating Council.* The SCC consists of representatives of 28 nongovernment entities, most of which are providers of voting systems and other election-related products and services. SCCs are self-organized and self-governed. They are intended to represent private-sector interests and to facilitate collaboration activities, including information sharing, among the private-sector entities in the CI sector and with government entities.

- *Sector-Specific Plan.* Public- and private-sector partners have created SSPs for each of the 16 CI sectors. There is also a plan for the State, Local, Tribal, and Territorial Government Coordinating Council. The plans are components of an overall National Infrastructure Protection Plan and provide a means for the sectors to establish goals and priorities for addressing risks. They are generally updated on a four-year cycle. The most recent versions were released in 2015 and therefore do not yet include the EIS.

The CI designation for election infrastructure is also intended to facilitate use of existing resources, such as

- *National Cybersecurity and Communications Integration Center.* The NCCIC is the primary federal focus for sharing CI cybersecurity.

- *Critical Infrastructure Partnership Advisory Council.* CIPAC provides election officials access to a broad range of relevant expertise and participation in sensitive planning conversations.

- *Multi-State Information Sharing and Analysis Center.* The MS-ISAC is one of the centers created to facilitate the sharing of security information for different CI sectors. It works with the NCCIC, all states, and many local governments to assist them in cybersecurity. The MS-ISAC supports the EIS-ISAC, created in 2018 to facilitate information-sharing activities for and among more than 500 members consisting of state and local election offices, as well as the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED).

Pursuant to the EIS designation, DHS and the EAC assisted both jurisdictions and vendors in preparations on election security for the 2018 federal election. For more information, see https://www.dhs.gov/topic/election-security, https://www.eac.gov/election-officials/elections-critical-infrastructure/, https://www.cisecurity.org/ei-isac/.

Why Was the Designation Initially Controversial?

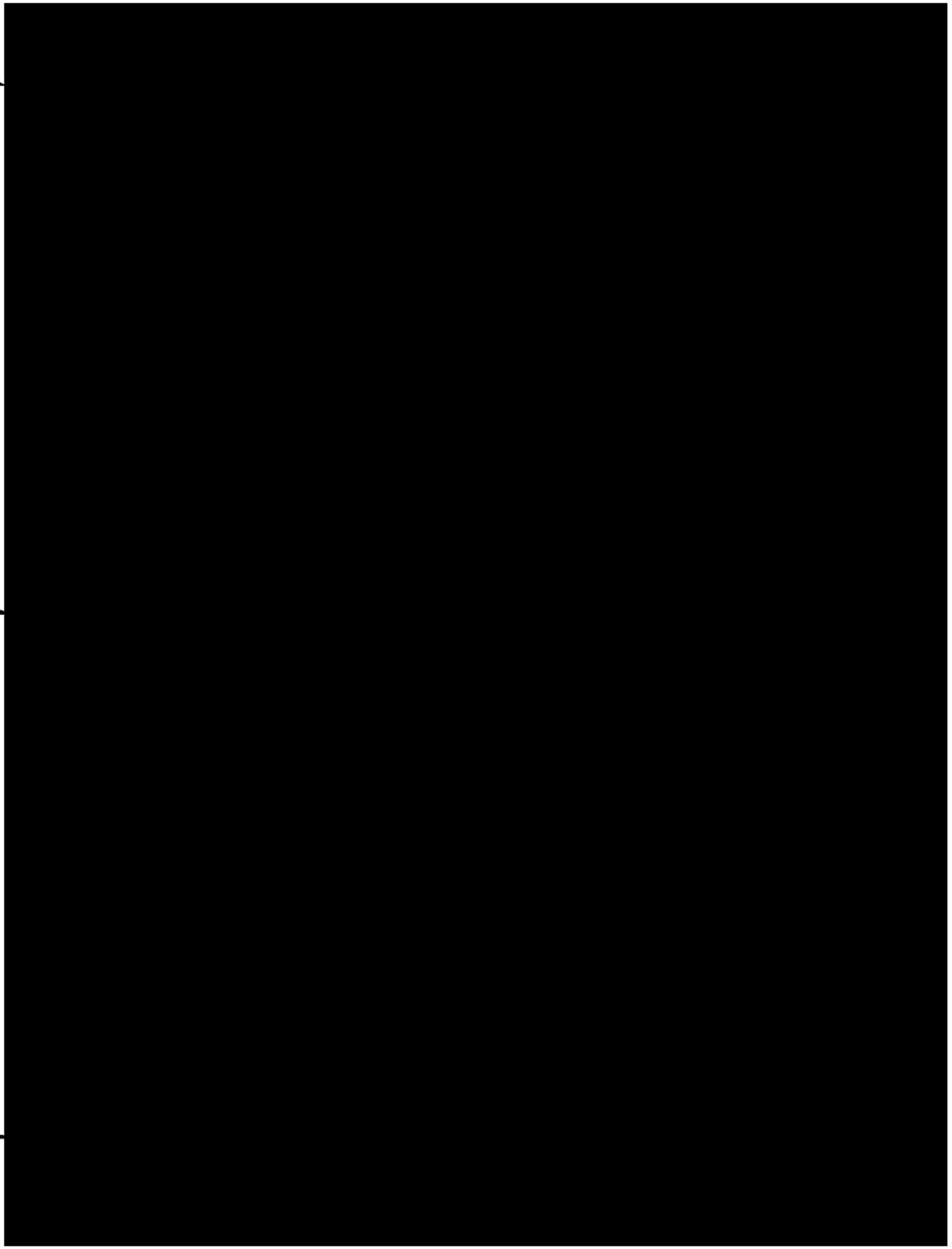
Misgivings about DHS involvement were raised when it first offered assistance to election jurisdictions in August 2016. Some observers feared that DHS would begin to exert control over the administration of elections or to engage in unrequested security activities.

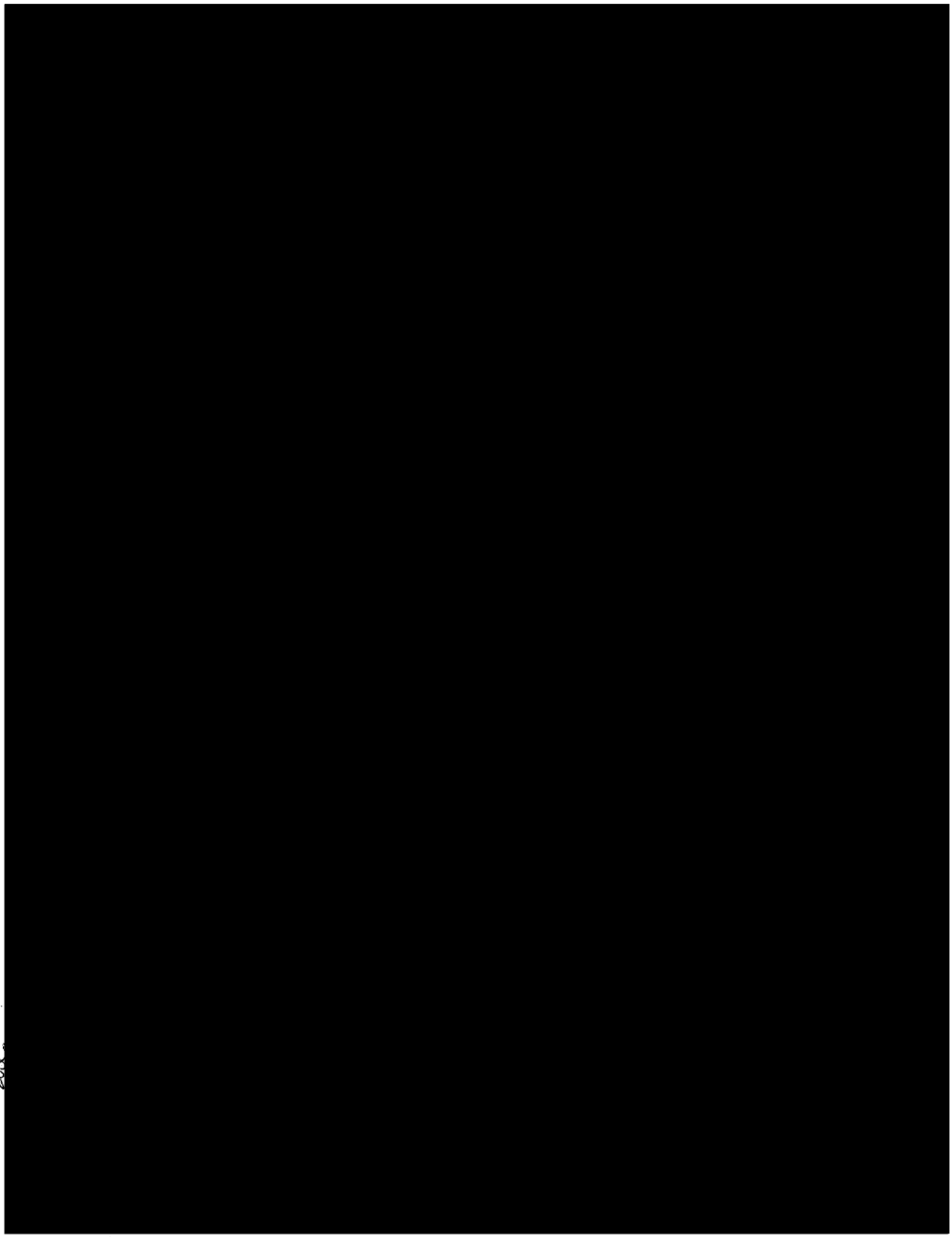
Controversy over the federal role in election administration is not new. Concerns about federal regulation of the election process were prominent during the legislative debate over HAVA and led to the inclusion of the regulatory restrictions in the law. Furthermore, bills in prior Congresses that would have provided DHS broad regulatory authority over cybersecurity have all failed.

The CI designation does not contravene the HAVA restrictions on EAC regulations or create DHS regulatory authority for the EIS. DHS provides assistance to election jurisdictions only on a voluntary basis. In the 115th Congress, a few bills would have established mandatory standards or federal rule-making authority, but none received committee or floor action. Bills with relevant provisions have also been introduced in the 116th Congress.

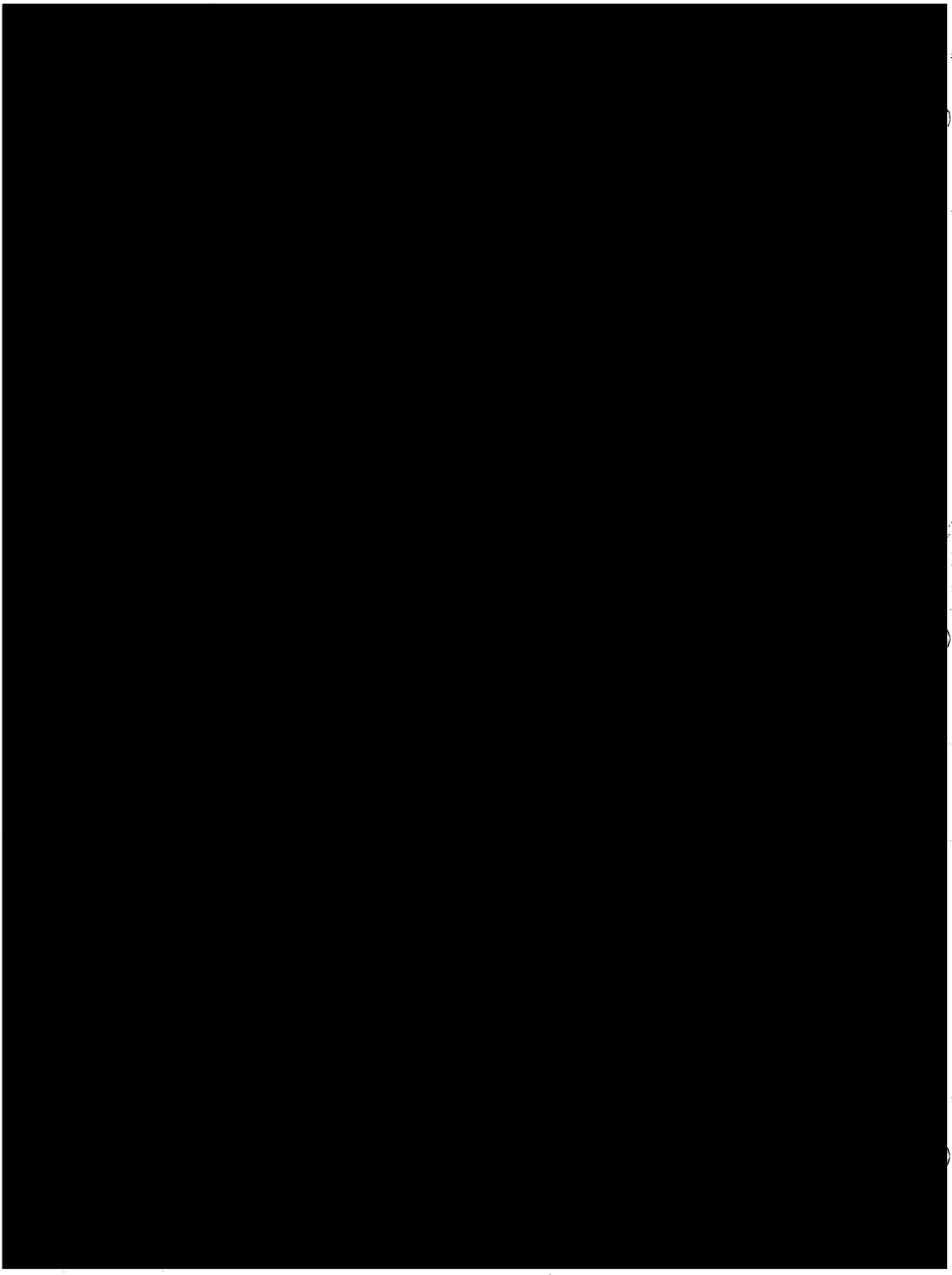
Eric A. Fischer, efischer@crs.loc.gov, 7-7071

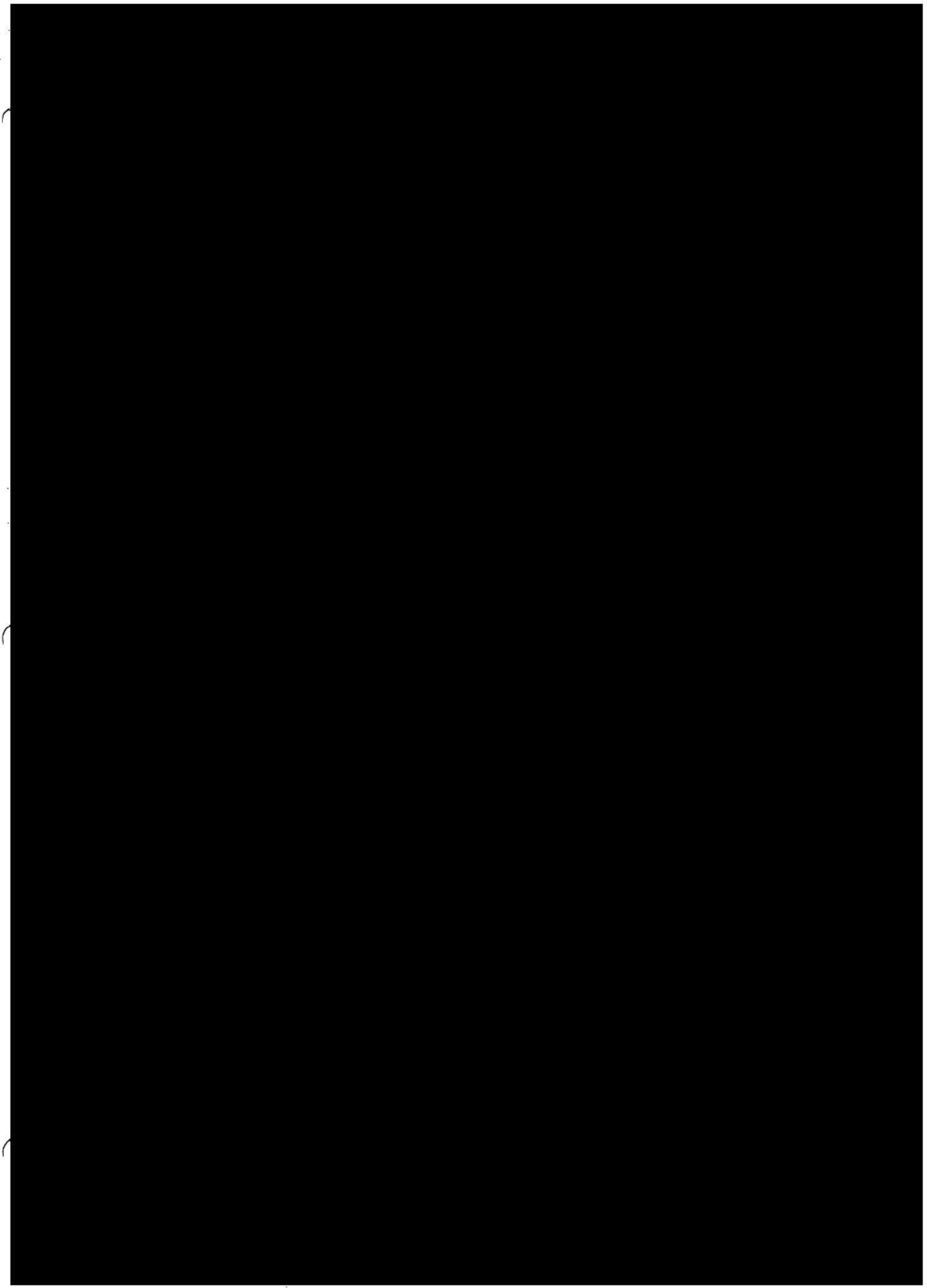
IF10677





[redacted]





From: Colleen McCormack
To: Bhanu Pothugunta
Subject: RE: 2FA - User Not Verified
Date: Thursday, November 29, 2018 2:47:16 PM

Bhanu,

I just had Debra Unger try and verify her text and email address. She did receive them both, but when she clicked on the link, she received "User Not Verified."

The email had the link hidden and the text does not have the link hidden. They both should be hidden.

Tomorrow I will be out of the office for a doctor appointment.

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, November 29, 2018 12:12 PM
To: Colleen McCormack
Subject: Re: 2FA - User Not Verified

Thank you colleen. We will work on this.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <colleen.mccormack@sos.nh.gov>
Sent: Thursday, November 29, 2018 11:58 AM
To: Bhanu Pothugunta
Subject: 2FA - User Not Verified

Bhanu,
I had Debra Unger try to use her email and she received the email, clicked on the link and received “user not verified”
Sheila Dodge tried to use text and she received the text, clicked on the link and received “user not verified”
They both have androids.
I will have Anthony try with his iphone now.

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel
To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: RE: 2FA - Verifying Cell Phone Number
Date: Tuesday, November 27, 2018 11:36:23 AM

Dan,

As discussed, we'll remove user information from the verification link and keep the encoded token number only. We'll update you once we move the change in UAT. Please let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, November 27, 2018 10:38 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: 2FA - Verifying Cell Phone Number

Perfect.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:37 AM
To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: Re: 2FA - Verifying Cell Phone Number

Ok. We'll call Dan at his direct line. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:35 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> It is a good time for us both.
> Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.
> Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,

Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> Can Dan and I call you back?
> He wants to discuss how the verification is coming back into ElectioNet?

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From:	Ganesh Veerabathiran
To:	Keval Patel; Daniel J Cloutier
Cc:	Colleen McCormack; Anthony Stevens; Bhanu Pothugunta
Subject:	RE: 2FA for ElectioNet
Date:	Tuesday, January 15, 2019 9:06:35 AM

Good morning Dan. Could you please add [redacted]" as the hostname on safe senders list.

Best Regards,
Ganesh Kumar Veerabathiran | Network Engineer
PCC Technology Inc., a subsidiary of GCR Inc. | pcctg.com
100 Northfield Dr. Suite 100 | Windsor, CT 06095
O. 860.580.7524

From: Keval Patel
Sent: Tuesday, January 15, 2019 8:22 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@sos.nh.gov>; Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: Re: 2FA for ElectioNet

Dan,

I've included Ganesh to call you on this. He is our IT manager and handles AWS email accounts. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jan 15, 2019, at 6:50 AM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Keval,
>
> We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.
>
> <image001.png>

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From:	Keval Patel
To:	Colleen McCormack
Cc:	Anthony Stevens; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject:	Re: 2-Factor Authentication CCR 2018-002
Date:	Monday, September 24, 2018 12:35:02 PM

Yes. I'll setup a call with you once we deploy. Also, we'll send release document. Thank you.

With Regards,

Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Sep 24, 2018, at 12:12 PM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval
> We are good to go now to deploy 2FA in UAT.
> Will it take some walking through the process with me?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, September 24, 2018 12:04 PM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta;

Sachin Shetty
Subject: RE: 2-Factor Authentication CCR 2018-002

Anthony,

Good morning. We are ready to deploy 2FA for NH SVRS in UAT. Please let me know when do you want me to deploy it in UAT. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

From:	Anand Balasubramanian
To:	Anthony Stevens; Keval Patel
Cc:	Colleen McCormack
Subject:	RE: CR No. 2018-002, Project No. 60042, Signed 5-15-2018 - ElectioNet Wallet Card as 2nd Factor
Date:	Wednesday, August 01, 2018 11:18:13 AM

https://www.yubico.com/

Anand Balasubramanian | CTO
GCR Inc. | GCRincorporated.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7245 | C. 860.833.7445

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Monday, July 30, 2018 2:55 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: RE: CR No. 2018-002, Project No. 60042, Signed 5-15-2018 - ElectioNet Wallet Card as 2nd Factor

Thanks, Keval.

We are available to talk this afternoon.

Anthony
(603)271-8238

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Saturday, July 28, 2018 3:43 PM
To: Anthony Stevens
Cc: Colleen McCormack; Anand Balasubramanian
Subject: Re: CR No. 2018-002, Project No. 60042, Signed 5-15-2018 - ElectioNet Wallet Card as 2nd Factor

Anthony,

Vishal has informed me about the discussion with you on this. Anand and I will call you on Monday to discuss with you in details. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jul 28, 2018, at 3:38 PM, Anthony Stevens <Anthony.Stevens@SOS.NH.GOV> wrote:

Keval,

At the NASS/NASED conference, I obtained more information at the PCC table on the wallet card approach to two-factor authentication. Using this approach, a wallet card would be separately programmed for each Electio*Net* user and then distributed to each user with a sign-off required. Wallet cards could be carried in the wallet of each Electio*Net* user and used at any time as the second factor identification for Electio*Net* log-in. Hence, in addition to accessing the second factor via cell phone and email, a third comparable mechanism would also be employed – the wallet card. The number for each user on their wallet card would be unique and would change quickly over time. It would be activated with the press of a button on a chip on the card.

I think the wallet card would be useful in the event that a user could not gain access to a text or email message. It seems to have been successful in a New Jersey rollout to 2,000 users.

Would you please advise me what it would cost to integrate the wallet card option into our existing change order for two-factor authentication, CR No. 2018-002, Project No. 60042, signed 5-15-2018? The cost should reflect the cost of purchasing wallet cards for all active Electio*Net* users, roughly 1,200.

Your people at the desk informed me that PCC had conducted a comparison of the various wallet cards available and their advantages and disadvantages. I think they mentioned that PCC could share that research with me. Kindly send to us whatever comparative analysis you have that might be useful, as well as your recommended product.

Thank you.

Anthony Stevens
Assistant Secretary of State
71 S. Fruit St.
Concord
New Hampshire 03301
Tel: (603)271-8238

From:	Condos, Jim
To:	William Gardner; Denise Merrill (CT) (denise.merrill@ct.gov); Matthew Dunlap (matthew.dunlap@maine.gov); William Galvin; Nellie Gorbea (nmgorbea@sos.ri.gov)
Cc:	Moriah Moriarty; Scott Bates; Peggy Reeves; Laura Supica; Dottie Canelli (dorothy.canelli@maine.gov); Julie Flynn (julie.flynn@maine.gov); Michelle.Tassinari@sec.state.ma.us; Betty Sepe; Rob Rock; Gonzalo Cuervo; Karen Ladd; Anthony Stevens; Paula Penney; Covey, Eric; Winters, Chris; Senning, Will
Subject:	RE: DHS Hosts New England Regional State Election Security Forum - June 11-12, 2019 - Found word(s) not intended in the Text body
Date:	Thursday, May 16, 2019 3:52:58 PM

Sorry Bill - you will be missed...
If you can send some of your team, it is only an hour away!
VT is sending some of its State Police Intel Officers as well as some of its IT Security folks.

-----Original Message-----
From: William Gardner <wgardner@sos.nh.gov>
Sent: Tuesday, May 14, 2019 1:53 PM
To: Condos, Jim <jim.condos@sec.state.vt.us>; Denise Merrill (CT) (denise.merrill@ct.gov) <denise.merrill@ct.gov>; Matthew Dunlap (matthew.dunlap@maine.gov) <matthew.dunlap@maine.gov>; William Galvin <nancy.driscoll@sec.state.ma.us>; Nellie Gorbea (nmgorbea@sos.ri.gov) <nmgorbea@sos.ri.gov>
Cc: Moriah Moriarty <Moriah.Moriarty@ct.gov>; Scott Bates <Scott.Bates@ct.gov>; Peggy Reeves <Peggy.Reeves@ct.gov>; Laura Supica <Laura.Supica@maine.gov>; Dottie Canelli (dorothy.canelli@maine.gov) <dorothy.canelli@maine.gov>; Julie Flynn (julie.flynn@maine.gov) <julie.flynn@maine.gov>; Michelle.Tassinari@sec.state.ma.us; Betty Sepe <bsepe@sos.ri.gov>; Rob Rock <rrock@sos.ri.gov>; Gonzalo Cuervo <gcuervo@sos.ri.gov>; Karen Ladd <Karen.Ladd@SOS.NH.GOV>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Paula Penney <Paula.Penney@SOS.NH.GOV>; Covey, Eric <eric.covey@sec.state.vt.us>; Winters, Chris <chris.winters@sec.state.vt.us>; Senning, Will <will.senning@sec.state.vt.us>
Subject: Re: DHS Hosts New England Regional State Election Security Forum - June 11-12, 2019 - Found word(s) not intended in the Text body

Unfortunately there was no prior discussion about the timing of this event. Mid-June is a critical point in time in our legislative session that requires my office's full attention to its constitutional legislative duties. As a result, it's not possible for me or any of my staff to attend.

Best,

Bill

_____
From: Condos, Jim <jim.condos@sec.state.vt.us>
Sent: Tuesday, May 14, 2019 1:35:16 PM
To: Denise Merrill (CT) (denise.merrill@ct.gov); Matthew Dunlap (matthew.dunlap@maine.gov); William Galvin; William Gardner; Nellie Gorbea (nmgorbea@sos.ri.gov)
Cc: Moriah Moriarty; Scott Bates; Peggy Reeves; Laura Supica; Dottie Canelli (dorothy.canelli@maine.gov); Julie Flynn (julie.flynn@maine.gov); Michelle.Tassinari@sec.state.ma.us; Betty Sepe; Rob Rock; Gonzalo Cuervo; Karen Ladd; Anthony Stevens; Paula Penney; Covey, Eric; Winters, Chris; Senning, Will
Subject: RE: DHS Hosts New England Regional State Election Security Forum - June 11-12, 2019

Hi NE Secs…

Hope you are all planning on sending a team to this important event in June.

Bill, it is scheduled in your state.

[cid:image001.png@01D50A59.DC93F9B0]

From: Reynolds, Leslie <reynolds@sso.org>
Sent: Tuesday, May 14, 2019 12:55 PM
To: Denise Merrill (CT) (denise.merrill@ct.gov) <denise.merrill@ct.gov>; Matthew Dunlap (matthew.dunlap@maine.gov) <matthew.dunlap@maine.gov>; William Galvin <nancy.driscoll@sec.state.ma.us>; William Gardner (wgardner@sos.state.nh.us) <wgardner@sos.state.nh.us>; Condos, Jim <jim.condos@sec.state.vt.us>; Nellie Gorbea (nmgorbea@sos.ri.gov) <nmgorbea@sos.ri.gov>
Cc: Moriah Moriarty <Moriah.Moriarty@ct.gov>; Scott Bates <Scott.Bates@ct.gov>; Peggy Reeves <Peggy.Reeves@ct.gov>; Laura Supica <Laura.Supica@maine.gov>; Dottie Canelli (dorothy.canelli@maine.gov) <dorothy.canelli@maine.gov>; Julie Flynn (julie.flynn@maine.gov) <julie.flynn@maine.gov>; Michelle.Tassinari@sec.state.ma.us; Betty Sepe <bsepe@sos.ri.gov>; Rob Rock <rrock@sos.ri.gov>; Gonzalo Cuervo <gcuervo@sos.ri.gov>; kladd@sos.state.nh.us; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Paula Penney <ppenney@sos.state.nh.us>; Covey, Eric <eric.covey@sec.state.vt.us>; Winters, Chris <chris.winters@sec.state.vt.us>; Senning, Will <will.senning@sec.state.vt.us>
Subject: DHS Hosts New England Regional State Election Security Forum - June 11-12, 2019
Importance: High

Dear Secretaries:

On the Democracy History Tour last week, I received a few questions about the New England Regional State Election Security Forum. The invitees are the Secretaries and their staff from DHS Region I (CT, MI, MA, NH, RI and VT). As NASS President, they asked Sec. Condos to help them co-host this event which will take place at the University of NH in Durham. The event is June 11-12, 2019.

I offered to send the information out again, since I have easy access to the relevant email addresses. You can read the emails below from Sec. Condos and DHS. Attached you will find the agenda and invite. While the deadline has passed, I am sure that late registrants are welcome.

Please RSVP to IPRegion1@hq.dhs.gov<mailto:IPRegion1@hq.dhs.gov>. Please direct any questions to Tracy Shawyer at 202-870-7698. This is NOT a NASS event, thus I will not have any answers to your questions☺

Best,
Leslie

Leslie Reynolds
Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street, NW Suite 401
Washington, DC 20001
202-624-3525
https://urldefense.proofpoint.com/v2/url?u=http-3A__www.nass.org&d=DwIGaQ&c=WZLRWjmU0vQ6jkmOu6nAYA&r=-v22NTeHrtBDOtEKIDCk7IdohPYElD9iX-tOFMDUCx0&m=GptDXBHuf5NbhIrf7k6OsG_za8insr97JcPig4Jhab8&s=u1uiDocc5KRggajbkY0E2ZQJtN4DLS5HRJLU5G3JFI8&e=
<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.nass.org&d=DwMGaQ&c=WZLRWjmU0vQ6jkmOu6nAYA&r=hrGu146eUHyQNim5nL_DSOy3-idnvmXsi6hDZbkGGbY&m=GILKWMawFl1LnCq6yZlMW9lBTmsxKfCX66FGHseiO2w&s=M3CURWbcjczfZm3lOvYTsDdfIndAkTMatGquALRq0Wk&e=>

From: McCann, Matthew [mailto:matthew.mccann@hq.dhs.gov]
Sent: Friday, March 22, 2019 9:51 AM
To: Condos, Jim <jim.condos@sec.state.vt.us<mailto:jim.condos@sec.state.vt.us>>; denise.merrill@ct.gov<mailto:denise.merrill@ct.gov>; moriah.moriarty@ct.gov<mailto:moriah.moriarty@ct.gov>; matthew.dunlap@me.gov<mailto:matthew.dunlap@me.gov>; Laura.Supica@maine.gov<mailto:Laura.Supica@maine.gov>; nancy.driscoll@sec.state.ma.us<mailto:nancy.driscoll@sec.state.ma.us>; wgardner@sos.state.nh.us<mailto:wgardner@sos.state.nh.us>; ppenney@sos.state.nh.us<mailto:ppenney@sos.state.nh.us>; nmgorbea@sos.ri.gov<mailto:nmgorbea@sos.ri.gov>; bsepe@sos.ri.gov<mailto:bsepe@sos.ri.gov>; 'denise.merrill@ct.gov' <denise.merrill@ct.gov<mailto:denise.merrill@ct.gov>>; 'jim.condos@sec.state.vt.us' <jim.condos@sec.state.vt.us<mailto:jim.condos@sec.state.vt.us>>; 'will.senning@sec.state.vt.u' <will.senning@sec.state.vt.u<mailto:will.senning@sec.state.vt.u>>; 'scott.bates@ct.gov' <scott.bates@ct.gov<mailto:scott.bates@ct.gov>>; 'Peggy.Reeves@ct.gov' <Peggy.Reeves@ct.gov<mailto:Peggy.Reeves@ct.gov>>; 'matthew.dunlap@maine.gov' <matthew.dunlap@maine.gov<mailto:matthew.dunlap@maine.gov>>; 'donna.e.grant@maine.gov' <donna.e.grant@maine.gov<mailto:donna.e.grant@maine.gov>>; 'julie.flynn@maine.gov' <julie.flynn@maine.gov<mailto:julie.flynn@maine.gov>>; 'nmgorbea@sos.ri.gov' <nmgorbea@sos.ri.gov<mailto:nmgorbea@sos.ri.gov>>; 'nlagace@sos.ri.gov' <nlagace@sos.ri.gov<mailto:nlagace@sos.ri.gov>>; 'Michelle.Tassinari@sec.state.ma.us' <Michelle.Tassinari@sec.state.ma.us<mailto:Michelle.Tassinari@sec.state.ma.us>>; 'daniel.cloutier@sos.nh.gov' <daniel.cloutier@sos.nh.gov<mailto:daniel.cloutier@sos.nh.gov>>; 'keryn.cadogan@state.ma.us' <keryn.cadogan@state.ma.us<mailto:keryn.cadogan@state.ma.us>>; 'chris.winters@sec.state.vt.us' <chris.winters@sec.state.vt.us<mailto:chris.winters@sec.state.vt.us>>; 'debra.o'malley@state.ma.us' <debra.o'malley@state.ma.us>; Covey, Eric <eric.covey@sec.state.vt.us<mailto:eric.covey@sec.state.vt.us>>; Plummer, Perry <perry.plummer@dos.nh.gov<mailto:perry.plummer@dos.nh.gov>>; 'Farnham, Douglas A Brig Gen USAF NG MEANG (US)' <douglas.a.farnham.mil@mail.mil<mailto:douglas.a.farnham.mil@mail.mil>>; 'kevin.lane@vt.gov' <kevin.lane@vt.gov<mailto:kevin.lane@vt.gov>>; 'Dora.Schriro@ct.gov' <Dora.Schriro@ct.gov<mailto:Dora.Schriro@ct.gov>>; 'Mike.Steinmetz@governor.ri.gov' <Mike.Steinmetz@governor.ri.gov<mailto:Mike.Steinmetz@governor.ri.gov>>; Herrick, Christopher <Christopher.Herrick@vermont.gov<mailto:Christopher.Herrick@vermont.gov>>; Jeanne Benincasa (jeanne.benincasa@state.ma.us<mailto:jeanne.benincasa@state.ma.us>) <jeanne.benincasa@state.ma.us<mailto:jeanne.benincasa@state.ma.us>>; 'Suzanne.Krauss@maine.gov' <Suzanne.Krauss@maine.gov<mailto:Suzanne.Krauss@maine.gov>>
Cc: Lindsey Forson <lforson@sso.org<mailto:lforson@sso.org>>; Reynolds, Leslie <reynolds@sso.org<mailto:reynolds@sso.org>>; Shawyer, Tracy <tracy.shawyer@hq.dhs.gov<mailto:tracy.shawyer@hq.dhs.gov>>; Modricker, Daniel <daniel.modricker@hq.dhs.gov<mailto:daniel.modricker@hq.dhs.gov>>; Masterson, Matthew <matthew.masterson@hq.dhs.gov<mailto:matthew.masterson@hq.dhs.gov>>; Bailey, Timothy <timothy.bailey@HQ.DHS.GOV<mailto:timothy.bailey@HQ.DHS.GOV>>; MARKS STEPHEN A <stephen.marks@usss.dhs.gov<mailto:stephen.marks@usss.dhs.gov>>; gmmcmahon@fbi.gov<mailto:gmmcmahon@fbi.gov>; Dean, Paul <Paul.Dean@unh.edu<mailto:Paul.Dean@unh.edu>>; IP Region 1 PSA <IPRegion1PSA@hq.dhs.gov<mailto:IPRegion1PSA@hq.dhs.gov>>; Rossi, Richard <Richard.rossi@hq.dhs.gov<mailto:Richard.rossi@hq.dhs.gov>>; Ford, Ron <ron.ford@hq.dhs.gov<mailto:ron.ford@hq.dhs.gov>>; Snell, Allison <Allison.Snell@HQ.DHS.GOV<mailto:Allison.Snell@HQ.DHS.GOV>>; Breor, Scott <scott.breor@hq.dhs.gov<mailto:scott.breor@hq.dhs.gov>>
Subject: New England Regional State Election Security Forum
Importance: High

Greetings All,

As per the below 'Save the Date' email from co-host Secretary Condos sent to the Secretaries of States, we are pleased to invite you to an inaugural New England Regional State Election Security Forum on 11-12 June. This event is intended to provide a collaborative opportunity for State Election Officials, CISOs, State HSAs, and pertinent Federal partners to discuss election security dynamics. The superb meeting venue is graciously being provided by the University of New Hampshire.

This forum will enable us all to take advantage of the momentum from the 2018 mid-term elections, share collective best practices/lessons learned, and align stakeholder requirements as we head into the 2020 general election cycle. For State Election Officials… this event is not intended to replace or revisit meetings held with NASS and/or the DHS Election Task Force within the National Capital Region.

Please note this event will be closed to media. If amenable to participants, a collective press release can be crafted by CISA and issued post-event. We can likewise arrange for a post-event media engagement opportunity, but will do so only if there is expressed interest from the participating states.

The draft agenda and invite are attached for your reference. A finalized agenda and other logistical information will follow soon. Should you have any questions and/or event-related recommendations, feel free to email us at IPRegion1@hq.dhs.gov<mailto:IPRegion1@hq.dhs.gov> or contact Tracy Shawyer at 202-870-7698.

Request your RSVPs be provided to IPRegion1@hq.dhs.gov<mailto:IPRegion1@hq.dhs.gov>, preferably by May 10th. Looking forward to seeing everyone!

Best,
Matt

Matt McCann
Regional Director, Region 1 – New England Cybersecurity and Infrastructure Security Agency US Department of Homeland Security

matthew.mccann@hq.dhs.gov<mailto:matthew.mccann@hq.dhs.gov>
(c) 617-840-5469
[cid:image001.png@01D4C511.63C50840]

From: Condos, Jim <jim.condos@sec.state.vt.us<mailto:jim.condos@sec.state.vt.us>>
Sent: Thursday, February 28, 2019 3:09 PM
To: denise.merrill@ct.gov<mailto:denise.merrill@ct.gov>; moriah.moriarty@ct.gov<mailto:moriah.moriarty@ct.gov>; matthew.dunlap@me.gov<mailto:matthew.dunlap@me.gov>; Laura.Supica@maine.gov<mailto:Laura.Supica@maine.gov>; nancy.driscoll@sec.state.ma.us<mailto:nancy.driscoll@sec.state.ma.us>; wgardner@sos.state.nh.us<mailto:wgardner@sos.state.nh.us>; ppenney@sos.state.nh.us<mailto:ppenney@sos.state.nh.us>; nmgorbea@sos.ri.gov<mailto:nmgorbea@sos.ri.gov>; bsepe@sos.ri.gov<mailto:bsepe@sos.ri.gov>
Cc: Lindsey Forson <lforson@sso.org<mailto:lforson@sso.org>>; Reynolds, Leslie <reynolds@sso.org<mailto:reynolds@sso.org>>; Winters, Chris <chris.winters@sec.state.vt.us<mailto:chris.winters@sec.state.vt.us>>; Covey, Eric <eric.covey@sec.state.vt.us<mailto:eric.covey@sec.state.vt.us>>; McCann, Matthew <matthew.mccann@hq.dhs.gov<mailto:matthew.mccann@hq.dhs.gov>>; Shawyer, Tracy <tracy.shawyer@hq.dhs.gov<mailto:tracy.shawyer@hq.dhs.gov>>; Donnelly, Timothy <Timothy.Donnelly@hq.dhs.gov<mailto:Timothy.Donnelly@hq.dhs.gov>>
Subject: SAVE THE DATE: 6/11 - 6/12/19 --- New England Region SoS Cyber Security Opportunity

Please see the attached…

This is a SAVE THE DATE for an exciting opportunity that DHS Region 1 (New England) Director, Matt McCann and I have discussed to review the 2018 Election and begin preparing for the 2020 Election

This will be open to each of the New England states and we can invite up to 8 people to attend.
The following information and the attached invitation should cover the basics.

What: Election Officials Regional Forum
When: 11-12 June 2019. Start time is 10:30am on 11 June and the event will end at 4:00pm on 12 June.
Where: University of New Hampshire, Holloway Commons Conference Center, 83 Main Street, Durham NH 03824
How: Partnership between DHS/CISA Region 1 and NASS President/Vermont Secretary of State.
Who: Each New England state is welcome to bring up to eight representatives with recommended participants to include the:

Secretary,

Deputy Secretary,

Chief of Staff,

Elections Director,

CISO,

IT Manager, and

Homeland Security Advisor.

Additionally, federal entities beyond DHS/CISA involved in election security related activities such as DHS Intelligence & Analysis, the U.S. Secret Service, and the Federal Bureau of Investigation will participate.

Why:

A timely opportunity to capture the momentum from the 2018 election cycle, share best practices/lessons learned, and better understand stakeholders requirements as we head into the 2020 general election cycle.

The collaborative format will lay the groundwork for developing a clear path forward on optimally coordinating on election security and resilience efforts.

The forum will enable information sharing about cybersecurity risks, voluntary resources, and technical assistance options.

In order to help stakeholders better assess potential threats, intelligence community representatives will provide the latest threat picture.

Stakeholders recognize that securing our nation's election infrastructure is a shared responsibility and we are seeking to further leverage partnerships to advance that mission.

Please review and decide who you will invite and respond to the contact on the attached Invite.
More information to follow with the agenda and other logistics information.

[cid:image003.png@01D4DFE7.178468E0]

From: Colleen McCormack
To: Keval Patel; Bhanu Pothugunta
Subject: RE: Discussion on Statewide checklist report
Date: Thursday, August 30, 2018 4:07:56 PM
Attachments: image001.png

Keval,

I forgot to ask them. We have been out of the office and at meetings. They are both out of the office today.

I will ask them tomorrow, so you may code the retention period properly.

Thank you for reminding me.

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Thursday, August 30, 2018 4:03 PM
To: Colleen McCormack; Bhanu Pothugunta
Subject: RE: Discussion on Statewide checklist report

Colleen,

Did you check with Dan and Anthony on the retention period for this reports? Size is our problem so we need to have some sort of clean-up process. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, August 30, 2018 4:01 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>
Subject: RE: Discussion on Statewide checklist report

Bhanu,
The statewide checklist report was tested in UAT and it passed. Thank you for updating the wards.
Can you move this to production after 9:00 PM tonight?
Or when is a better time for you?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, August 30, 2018 10:13 AM
To: Colleen McCormack; Keval Patel
Subject: RE: Discussion on Statewide checklist report

Colleen,

I have moved this fix to UAT. The report ID 000000004 in scheduler report status page was generated by ward.Please review and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687

M: 860.752.3834

From: Bhanu Pothugunta
Sent: Tuesday, August 28, 2018 7:26 AM
To: Colleen McCormack <colleen.mccormack@sos.nh.gov>; Keval Patel <Keval.Patel@pcctg.com>
Subject: Re: Discussion on Statewide checklist report

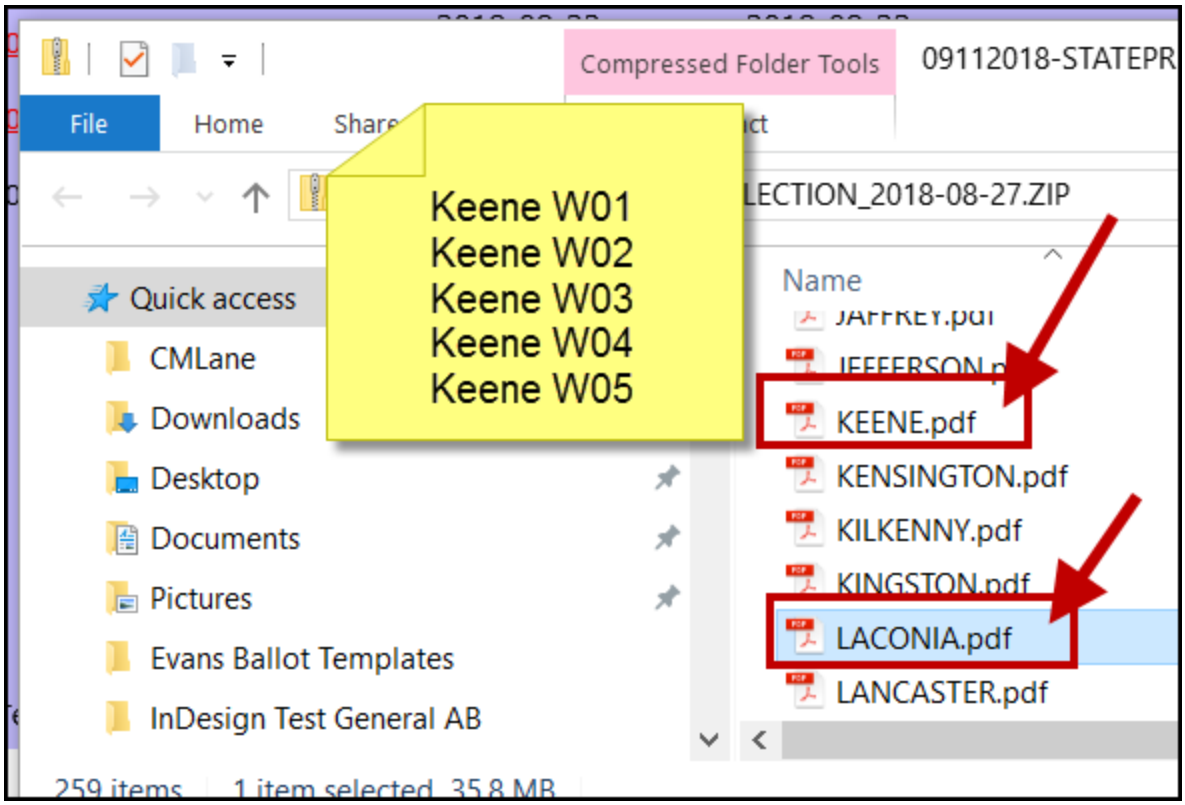
Colleen,

We will work on this and update you. Thank you.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <colleen.mccormack@sos.nh.gov>
Sent: Tuesday, August 28, 2018 7:20 AM
To: Bhanu Pothugunta; Keval Patel
Subject: RE: Discussion on Statewide checklist report

Bhanu,
The zip file was downloaded this morning and most of the towns looked correct.
We need each city or town that has wards to download separately by each ward and named as such. Currently the towns or cities that have wards are one PDF and the wards are merged together by alpha.
City of Keene has 5 wards.
City of Laconia has 6 wards, etc.



Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Monday, August 27, 2018 4:39 PM
To: Colleen McCormack; Keval Patel

Subject: RE: Discussion on Statewide checklist report

Thank You Colleen.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, August 27, 2018 4:37 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>
Subject: RE: Discussion on Statewide checklist report

Bhanu,
I just rescheduled the statewide report and it was successful.
I will look there tomorrow morning for the report.
Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Monday, August 27, 2018 2:32 PM
To: Colleen McCormack; Keval Patel
Subject: RE: Discussion on Statewide checklist report

Colleen,

Can you try to schedule it now and let me know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

-----Original Appointment-----
From: Bhanu Pothugunta
Sent: Monday, August 27, 2018 11:38 AM
To: Colleen.McCormack@sos.nh.gov; Keval Patel
Subject: Discussion on Statewide checklist report
When: Monday, August 27, 2018 2:00 PM-2:30 PM (UTC-05:00) Eastern Time (US & Canada).
Where:

-- Do not delete or change any of the following text. --

Join Webex meeting

Meeting number (access code): 794 455 948
Meeting password: mEwGsfH6

Join by phone

+1-650-429-3300 Call-in toll number (US/Canada)

Global call-in numbers

Can't join the meeting?

If you are a host, go here to view host information.

IMPORTANT NOTICE: Please note that this Webex service allows audio and other information sent during the session to be recorded, which may be discoverable in a legal matter. By joining this session, you automatically consent to such recordings. If you do not consent to being recorded, discuss your concerns with the host or do not join the session.

From: Bhanu Pothugunta
To: Colleen McCormack
Cc: Keval Patel
Subject: RE: ElectioNet - 2FA New Wording
Date: Thursday, April 18, 2019 2:07:33 PM

Colleen,

I have fixed this in UAT. Please review and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, April 17, 2019 3:05 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet - 2FA New Wording

Bhanu,
I have attached the new wording for the email/mobile verification and authentication messages.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: ElectioNet - 2FA UAT
Date: Thursday, March 21, 2019 12:41:08 PM

Okay that works. Thank You.

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, March 21, 2019 12:40 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: ElectioNet - 2FA UAT

No, there is no one.
No worries. I will test it when I come back.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, March 21, 2019 12:27 PM
To: Colleen McCormack
Subject: Re: ElectioNet - 2FA UAT

Colleen,

We are working on it we will release the fix tonight as there is UAT training going on. Is there any one from your office can test this??

Thank you.

Regards,
Bhanu Pothugunta

O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <colleen.mccormack@sos.nh.gov>
Sent: Thursday, March 21, 2019 12:23 PM
To: Bhanu Pothugunta
Subject: ElectioNet - 2FA UAT

Bhanu,
I was able to log into UAT this morning without being asked for a code to authenticate.

I reported this in the PCC TAS ticket.

Maybe one hour later, I was logging into UAT again and it asked me for a code.

Is the internal clock running exactly 24 hours (1 day) from the time I set/save the timing for the remembered device? Perhaps this is the issue? Can we have it expire at 2AM of the day it is meant to expire?

A reminder, I will not be in the office starting tomorrow. I will be back in the office on Monday April 1st.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Keval Patel; Bhanu Pothugunta
Cc: Daniel J Cloutier; Anthony Stevens
Subject: RE: ElectioNet - E Poll Books
Date: Monday, March 11, 2019 2:50:01 PM

Keval,

Wednesday or Thursday after 2PM is good either day for me.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, March 11, 2019 1:43 PM
To: Colleen McCormack; Bhanu Pothugunta
Cc: Daniel J Cloutier; Anthony Stevens
Subject: RE: ElectioNet - E Poll Books

Colleen,

We need to discuss on this to understand the scope of work for PCC. Please let me know if you are available this Wednesday or Thursday after 2pm. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, March 11, 2019 1:40 PM

To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: ElectioNet - E Poll Books

Keval,

We have a possible vendor that will be certified for e poll books. The certification will be for Voter History, Name changes and address changes. At this time, it will not capture new voter registrations.
We have a pilot for one NH town tomorrow.
We need to know the process for uploading these fields from the e poll books.

We need all of the fields captured on the marked checklist, Election Name, Voter ID,LN, FN, MN and suffix , party, domicile address, mailing address, CVA (yes or no) and absentee or regular ballot. Plus if the voter presented an Out of State Driver's License, which is now captured in a different screen other than batch input.

Let me know your thoughts on this process.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel
To: Daniel J Cloutier; Colleen McCormack; Bhanu Pothugunta; Sachin Shetty
Cc: Anthony Stevens
Subject: RE: ElectioNet - E Poll Books
Date: Friday, March 29, 2019 1:32:28 PM

Dan,

Below is our high level estimate for ePollBook data upload. I'll provide detailed SOW once you approve the estimate. Please review and let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Monday, March 25, 2019 2:53 PM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: RE: ElectioNet - E Poll Books

Keval,

Any news on the subject of uploaded data from an ePollBook?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, March 11, 2019 2:50 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: RE: ElectioNet - E Poll Books

Keval,

Wednesday or Thursday after 2PM is good either day for me.

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, March 11, 2019 1:43 PM
To: Colleen McCormack; Bhanu Pothugunta
Cc: Daniel J Cloutier; Anthony Stevens
Subject: RE: ElectioNet - E Poll Books

Colleen,

We need to discuss on this to understand the scope of work for PCC. Please let me know if you are available this Wednesday or Thursday after 2pm. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, March 11, 2019 1:40 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: ElectioNet - E Poll Books

Keval,

We have a possible vendor that will be certified for e poll books. The certification will be for Voter History, Name changes and address changes. At this time, it will not capture new voter registrations.
We have a pilot for one NH town tomorrow.
We need to know the process for uploading these fields from the e poll books.

We need all of the fields captured on the marked checklist, Election Name, Voter ID,LN, FN, MN and suffix , party, domicile address, mailing address, CVA (yes or no) and absentee or regular ballot. Plus if the voter presented an Out of State Driver's License, which is now captured in a different screen other than batch input.

Let me know your thoughts on this process.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: John Penney; Colleen McCormack
Subject: RE: ElectioNet - Statewide Checklist
Date: Friday, October 19, 2018 9:21:32 AM
Attachments: image001.png
image002.png

Thank You John.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: John Penney <John.Penney@SOS.NH.GOV>
Sent: Friday, October 19, 2018 8:07 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: ElectioNet - Statewide Checklist

Bhanu,

Everything looks good. Thank you for getting things to work again!

JOHN PENNEY
Technical Support Specialist
NH Department of State
Phone: 603-271-8852
E-mail: John.Penney@sos.nh.gov

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Friday, October 19, 2018 7:41 AM
To: Colleen McCormack
Cc: John Penney
Subject: RE: ElectioNet - Statewide Checklist

John,

Statewide rchecklist report has been generated last night. Please review and let me know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Bhanu Pothugunta
Sent: Thursday, October 18, 2018 9:45 AM
To: 'Colleen McCormack' <Colleen.McCormack@sos.nh.gov>
Cc: John Penney <John.Penney@SOS.NH.GOV>
Subject: RE: ElectioNet - Statewide Checklist

Sure Colleen. I will update him tomorrow for review. Thank You

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, October 18, 2018 9:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: John Penney <John.Penney@SOS.NH.GOV>
Subject: RE: ElectioNet - Statewide Checklist

Bhanu,
I will be away tomorrow, can you copy John Penney on the progress of the Statewide Checklist issue?
Thank you!

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, October 18, 2018 9:41 AM
To: Colleen McCormack
Subject: RE: ElectioNet - Statewide Checklist

Colleen,

I will look in to this and make sure that it will run tonight. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, October 18, 2018 8:10 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>

Subject: ElectioNet - Statewide Checklist

Bhanu,

The statewide checklist report has not run since 10/15/2018. Can you look into this for me?

☐	000000029	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	10/11/2018 01:00 AM	10/11/2018 02:01 AM	HD-CMCCOR	Viewed
☐	000000030	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	10/12/2018 01:00 AM	10/12/2018 02:01 AM	HD-CMCCOR	Viewed
☐	000000031	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	10/13/2018 01:00 AM	10/13/2018 02:03 AM	HD-CMCCOR	Viewed
☐	000000032	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	10/14/2018 01:00 AM	10/14/2018 02:02 AM	HD-CMCCOR	Viewed
☐	000000033	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	10/15/2018 01:00 AM		HD-CMCCOR	Ready For Proces

Delete Refresh Status

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: ElectioNet 2FA - Remembered Device
Date: Thursday, April 04, 2019 12:43:11 PM

Thank You Colleen. We will fix it. Thank You.

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, April 4, 2019 12:40 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: ElectioNet 2FA - Remembered Device

Bhanu,
The Remembered Device was tested and passed. It is now expiring at midnight. It is only the second user homepage screen that needs to be updated with "Verified" replacing "Remembered".

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Wednesday, April 03, 2019 11:56 AM
To: Colleen McCormack
Subject: RE: ElectioNet 2FA - Remembered Device

Sorry Colleen, We missed it. We will fix it.
Also I will send you the estimates for pending items by tomorrow. Thank You.

Regards,
Bhanu Pothugunta

O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, April 3, 2019 11:51 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: ElectioNet 2FA - Remembered Device

Bhanu,
You have updated on one of the user homepages "Mobile Device Verified" on the user's "My Information" screen.
The other screen is for the state users in "Maintain Users" and clicking on the user's name to view the "User Homepage" screen.
I will test the "Remembered Device" tomorrow morning.

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Wednesday, April 03, 2019 11:37 AM
To: Colleen McCormack
Subject: RE: ElectioNet 2FA - Remembered Device

Colleen,

We have fixed below items on UAT. Please review and let us know your comments. Thank You.

1. fix to expire at midnight of whatever day(s) timing is selected. (1, 2, 7, 14, 60, 90 days etc.)
2. User Homepage – change wording from "Mobile Device Remembered" to "Mobile Device Verified" & the same for "Email Device Verified."

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, April 3, 2019 11:01 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet 2FA - Remembered Device

Bhanu,
I have completed testing for the "Remembered Device" for the 2FA.

I had set the timing for one day for the device to be remembered.

ElectioNet works on a 24 hour clock.
The days should expire at midnight of whatever day(s) timing is selected.

I checked the box "Remember Device" at 10:24 AM yesterday on April 2nd.
I was able to log in today, April 3rd, without being asked for a code this morning at:
7:35 AM
8:38 AM
9:16 AM
10:23 AM
At 10:38 AM, I was asked for a code to authenticate.

Please fix this to expire at midnight of whatever day(s) timing is selected. (1, 2, 7, 14, 60, 90 days etc.)
User Homepage – change wording from "Mobile Device Remembered" to "Mobile Device Verified" & the same for "Email Device Verified."

What is the timing of the other outstanding tickets? Approximately.

Thank you Bhanu.

Thank You,

Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Bhanu Pothugunta
Subject: RE: ElectioNet Manage 2FA Settings Issue
Date: Thursday, January 17, 2019 12:05:56 PM

Thank you Bhanu, it has been corrected.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, January 17, 2019 12:00 PM
To: Colleen McCormack
Subject: RE: ElectioNet Manage 2FA Settings Issue

Colleen,

This is corrected now. Please review and let me know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, January 17, 2019 10:02 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: ElectioNet Manage 2FA Settings Issue

Bhanu,

The banner on the 2FA settings was not corrected.
It still reads: Mangage, instead of Manage

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, January 17, 2019 9:34 AM
To: Colleen McCormack
Subject: RE: ElectioNet Manage 2FA Settings Issue

Colleen,

This issue is fixed. Please review and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, January 16, 2019 4:00 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet Manage 2FA Settings Issue

Bhanu,
I am having an issue with saving one of the 2FA Settings.
Please see the attached document.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: ElectioNet Production - Statewide Checklist
Date: Wednesday, September 05, 2018 9:29:08 AM

Thank You Colleen.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, September 05, 2018 9:28 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: ElectioNet Production - Statewide Checklist

The download is complete. Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Wednesday, September 05, 2018 9:25 AM
To: Colleen McCormack
Subject: RE: ElectioNet Production - Statewide Checklist

Colleen,

Can you please try now. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Wednesday, September 05, 2018 8:39 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet Production - Statewide Checklist

Bhanu,

I ran my first statewide checklist in production last night and the file is empty. Could you please check on this for me?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Bhanu Pothugunta
Subject: RE: ElectioNet Production Statewide Checklist Issue
Date: Tuesday, September 18, 2018 3:43:42 PM
Attachments: image001.png

Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, September 18, 2018 3:43 PM
To: Colleen McCormack
Subject: RE: ElectioNet Production Statewide Checklist Issue

Colleen,

I will look in to this and update you. Tonight it will run at 12.00AM. Also I will monitor this schedule up to elections. Thank You

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, September 18, 2018 3:33 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet Production Statewide Checklist Issue

Bhanu,
I rescheduled the statewide checklist to run daily for the State General Election.
It has not completed since 9/14/2018.
Can you look into this for me?
See if I might have scheduled wrong???

☐	000000005	STATEWIDECHECKLIST	09/11/2018-STATE PRIMARY ELECTION	Daily	09/11/2018 11:00 PM	09/11/2018 11:54 PM	HD-CMCCOR	Viewed
☐	000000006	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	09/13/2018 12:00 AM	09/13/2018 08:33 AM	HD-CMCCOR	Viewed
☐	000000007	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	09/14/2018 12:00 AM	09/14/2018 12:56 AM	HD-CMCCOR	Viewed
☐	000000008	STATEWIDECHECKLIST	11/06/2018-STATE GENERAL ELECTION	Daily	09/15/2018 12:00 AM		HD-CMCCOR	Ready For Pro

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

STATEMENT OF CONFIDENTIALITY:
Any information contained in this electronic message or in any attachment to this message may contain confidential or privileged information and is intended for the exclusive use of the addressee(s). Please notify the Secretary of State's Office immediately at (603) 271-8241 or reply to nhvotes@sos.nh.gov if you are not the intended recipient and destroy all copies of this electronic message and any attachments.

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: ElectioNet Statewide Checklist
Date: Tuesday, November 13, 2018 10:18:51 AM
Attachments: image001.png

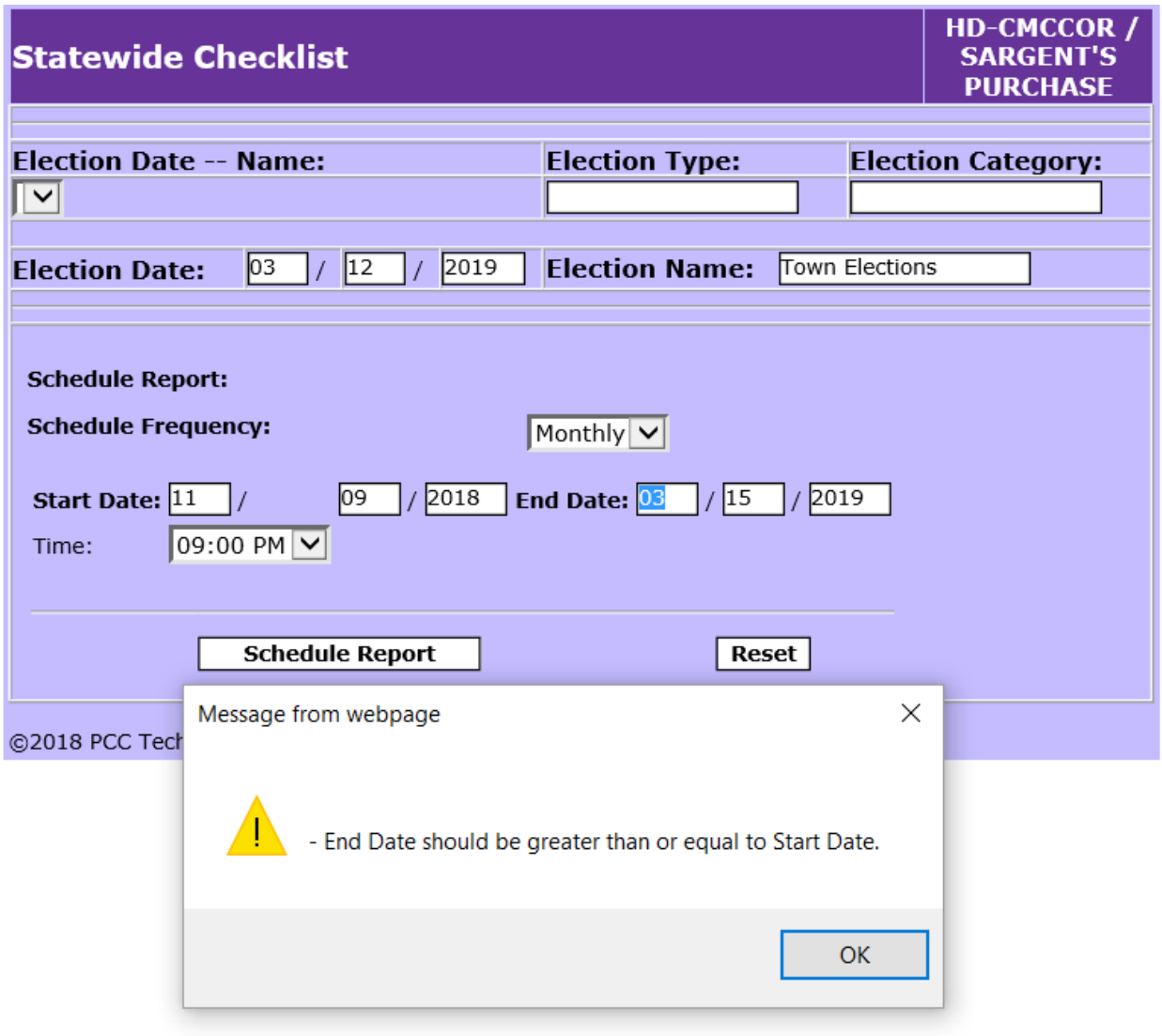
Colleen,

I have fixed this in UAT. Please review and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, November 08, 2018 9:17 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet Statewide Checklist

Bhanu,
I am trying to reschedule the statewide checklist to run once a month through March.
I am getting the pop up below. What am I not entering correctly for dates? Or is this an issue?



Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From:	Daniel J Cloutier
To:	Bhanu Pothugunta; Colleen McCormack
Subject:	RE: ElectioNet UAT - 2FA Issue
Date:	Tuesday, January 22, 2019 10:48:10 AM

I was just able to successfully authenticate using my uat test account.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, January 22, 2019 10:42 AM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

AWSProxy site was down for a while due to some firewall issue. Our IT administrator is looking into it. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 10:31 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: ElectioNet UAT - 2FA Issue

It is now working. What happened?

Thank You,
Colleen
Colleen E. McCormack

HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, January 22, 2019 10:26 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

It is working now. Can you please test and let me know if you are still having issues. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Bhanu Pothugunta
Cc: Keval Patel; Ganesh Veerabathiran; Michael Block; Anil Kumar Prathipati
Subject: RE: ElectioNet UAT Cannot Verify 2FA
Date: Tuesday, January 29, 2019 12:18:17 PM

Thank you Bhanu for monitoring the situation.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, January 29, 2019 12:17 PM
To: Colleen McCormack
Cc: Keval Patel; Ganesh Veerabathiran; Michael Block; Anil Kumar Prathipati
Subject: RE: ElectioNet UAT Cannot Verify 2FA

Colleen,

This issue is fixed now. There was a server patch update yesterday and it needs IIS to restart.
Going forward we will monitor the service and fix immediately as needed. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 29, 2019 9:00 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: ElectioNet UAT Cannot Verify 2FA

Bhanu,

We cannot receive any texts or emails for the 2FA authentication in UAT.

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Cc: Keval Patel
Subject: RE: New Password Screen Edit
Date: Saturday, June 15, 2019 12:41:04 PM

Colleen,

As discussed, I will move following items to production to night. Thank You.

1) Tas # 34964 - Password updates.
2) Tas # 34865 - Miscellaneous Updates to Screens and Pop ups
3) Tas # 34554 - Activities -> Maintain City/Town Data -> Election Officials changes

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

-----Original Message-----
From: Colleen McCormack <Colleen.McCormack@sos nh.gov>
Sent: Saturday, June 15, 2019 11:03 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>
Subject: Re: New Password Screen Edit

Bhanu,

I found an error in my counting of the password examples.

For the last example: [redacted]

It is only 23 characters long.

Can you update the blocked characters in the password to:

[redacted]

I added an "s" to the[redacted]

After this I believe I am done testing.

Thank you for being there on a weekend for me.

Thank You,
Colleen E. McCormack-Lane
HAVA
Department of State
State House, Room 204 - 107 North Main St Concord, NH 03301-4989 HAVA Office at 71 South Fruit St, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242
STATEMENT OF CONFIDENTIALITY:
Any information contained in this electronic message or in any attachment to this message may contain confidential or privileged information and is intended for the exclusive use of the addressee(s). Please notify the Secretary of State's Office immediately at (603) 271-3242 or reply to

nhvotes@sos.state.nh.us<https://owamail.sos.nh.gov/owa/redir.aspx?C=95138766a59e412ab224d09002730a29&URL=mailto%3anhvotes%40sos.state nh.us> if you are not the intended recipient and destroy all copies of this electronic message and any attachments.

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Saturday, June 15, 2019 8:37:27 AM
To: Colleen McCormack
Cc: Keval Patel
Subject: RE: New Password Screen Edit

Colleen,

I have moved the changes to UAT. Please review and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos nh.gov>
Sent: Thursday, June 13, 2019 3:50 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: New Password Screen Edit

Bhanu,
Here is the new wording for the change password screen.
I have come up with examples for our users of passwords or phrases that are easy to simulate.
Is there any way you can block these examples in the database that I have given?
Thus no one could type in the "exact" words and be able to save the password.
See attached.
[cid:image001.png@01D52355.8F30CCB0]

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St Concord, NH 03301-4989 ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Keval Patel; Bhanu Pothugunta; Anil Kumar Prathipati; Sachin Shetty
Subject: RE: NH 2FA Demo
Date: Wednesday, October 10, 2018 1:37:39 PM

I will be at lunch for about an hour.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

-----Original Message-----
From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Wednesday, October 10, 2018 12:55 PM
To: Bhanu Pothugunta; Colleen McCormack; Anil Kumar Prathipati; Sachin Shetty
Subject: RE: NH 2FA Demo

Colleen,

I am running late for our 1pm call. I'll call you once I finish the current meeting. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

-----Original Appointment-----
From: Bhanu Pothugunta
Sent: Wednesday, October 10, 2018 10:07 AM
To: Bhanu Pothugunta; Keval Patel
Subject: NH 2FA Demo
When: Wednesday, October 10, 2018 1:00 PM-2:00 PM Eastern Time.
Where: https://pcctg.webex.com/pcctg

JOIN WEBEX MEETING
https://pcctg.webex.com/pcctg/j.php?MTID=m1bc9fa508b9000090880f98d3be35754
Meeting number (access code): 798 564 390 Meeting password: Vr4GXcqc

JOIN BY IPHONE ONE-TAP
tel:+1-650-429-3300,,*01*798564390%23%23*01* Call-in toll number (US/Canada)

JOIN BY PHONE
+1-650-429-3300 Call-in toll number (US/Canada)

Global call-in numbers:
https://pcctg.webex.com/pcctg/globalcallin.php?serviceType=MC&ED=649519917&tollFree=0

Can't join the meeting?
https://collaborationhelp.cisco.com/article/WBX000029055

IMPORTANT NOTICE: Please note that this Webex service allows audio and other information sent during the session to be recorded, which may be discoverable in a legal matter. By joining this session, you automatically consent to such recordings. If you do not consent to being recorded, discuss your concerns with the host or do not join the session.

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: NH ElectioNet - 2FA Production
Date: Monday, June 03, 2019 10:55:46 AM

Colleen,

I will update it. And also will check what is the issue. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, June 3, 2019 10:51 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: NH ElectioNet - 2FA Production

Bhanu,
Are all the updates in ElectioNet Production that are currently in place for UAT for 2FA?
I just turned it on in Live and only enabled my user ID and I cannot get a text or email to go through to me.
This is huge, because sometimes there is no one in this office that can "disable" me from the 2FA.
Could you please disable me in Production?

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: Bhanu Pothugunta
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: NH ElectioNet - 2FA Updates
Date: Tuesday, November 27, 2018 12:45:10 PM

Thank you Bhanu.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, November 27, 2018 12:37 PM
To: Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: NH ElectioNet - 2FA Updates

Colleen,

I have created a TAS ticket(#33959). You can use this ticket to update issues/changes for 2FA.
We will work on the changes and update you. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, November 27, 2018 12:26 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: NH ElectioNet - 2FA Updates

Bhanu,

I have attached the updates needed in the 2FA process.

I did not add the ticket to TAS, so I cannot see the appropriate ticket number to report any issues. Could you tell me the ticket number, so I may document it.

Let me know if you have any questions.

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: RE: NH ElectioNet - 2FA
Date: Friday, June 07, 2019 12:02:39 PM

Thank You Colleen.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Friday, June 7, 2019 11:25 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: NH ElectioNet - 2FA

Bhanu,
The 2FA is working for me. I am having my office also test it.
Thank you!
Have a good weekend.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack; Keval Patel
Cc: Siva P. Nammi
Subject: RE: NH ElectioNet - Password Updates
Date: Thursday, June 13, 2019 2:06:54 PM

Colleen,

We will make the changes by tomorrow EOD and update you. I will send you an email and text once we moved the changes to UAT. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, June 13, 2019 1:14 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>
Subject: RE: NH ElectioNet - Password Updates

Thank you Bhanu,
Is it possible to make the change for the password reset by tomorrow? I can work this weekend to test if necessary, if that would help.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, June 13, 2019 1:10 PM
To: Colleen McCormack; Keval Patel
Subject: RE: NH ElectioNet - Password Updates

Colleen,

As users data in ERT is getting from Electionet, We need to do code changes in ERT as well to allow password length from 24 to 50 characters.
Currently ERT is allowing only 8 characters length. We will make the changes on ERT and update you.

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, June 13, 2019 10:45 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: NH ElectioNet - Password Updates

Correct. App does not need a user log in. It is a public website.

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Thursday, June 13, 2019 10:17 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: RE: NH ElectioNet - Password Updates

APP doesn't have user login. Correct?

I'll discuss with Bhanu and then call you today. Thank you.

With Regards,
Keval Patel | Assistant Vice President
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, June 13, 2019 10:16 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: NH ElectioNet - Password Updates

Keval,
When can we talk?
ERT users log in with their ElectioNet passwords.
Does this also effect APP website?

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Thursday, June 13, 2019 9:02 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: NH ElectioNet - Password Updates

Bhanu,

We need to talk more details on this. ERT needs to change also due to this change.

With Regards,
Keval Patel | Assistant Vice President
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jun 13, 2019, at 8:56 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> The updated password is working for UAT. I will do more testing for resetting a password.
> Checking UAT for APP website and ERT website, my IT person said the user table TX password did not copy over with the change of the password.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Thursday, June 13, 2019 4:20 AM
To: Colleen McCormack
Cc: Keval Patel
Subject: RE: NH ElectioNet - Password Updates

Colleen,

I have moved password changes to UAT except the eye ball in the password field. I will

work on this and update you.
Now all users in UAT should redirect to change password screen for one time.
Allowed special characters are `[!]@?#$%&()*+,-/:;<=>_`

Let me know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, June 11, 2019 7:48 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>
Subject: RE: NH ElectioNet - Password Updates

Bhanu
The deadline includes the updates to the 2FA screen also.
I was reviewing my documents and I just wanted to make sure I had told you it included the 2FA updates.
I have attached the latest update sent.

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Monday, June 10, 2019 4:54 PM
To: Colleen McCormack
Cc: Keval Patel

Subject: RE: NH ElectioNet - Password Updates

Colleen,

We will work on these changes and move it to UAT by Wednesday. Let me know if that works. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, June 10, 2019 4:27 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: NH ElectioNet - Password Updates

Bhanu,
I was just thinking the "reset password" button needs to be updated to generate a code of 24 random letters or numbers.
We are hoping this will be ready by the middle of the week. The projected start time for Production -2FA and new passwords is June 17th.
Will this be possible?
<image001.jpg><image002.jpg>

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]

Sent: Friday, June 07, 2019 4:23 PM
To: Colleen McCormack
Cc: Keval Patel
Subject: RE: NH ElectioNet - Password Updates

Colleen,

We will work on these changes and update you. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Friday, June 7, 2019 4:14 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: NH ElectioNet - Password Updates

Bhanu,
We are changing the passwords to be a minimum of 24 – 50 characters.
See the attached documents.
Logging into ElectioNet UAT with the new password configurations will be done all at once. Everyone will be asked to change their passwords.
AND I have some new wording for the 2FA screen where the user enters their code. See the attached document.
I am leaving the office at 4:30 PM. I will be back in the office on Monday at 7:AM. I have a meeting on Monday from 10:00 AM through 1:00 PM if you need to call me.
Have a good weekend.

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From:	Keval Patel
To:	Daniel J Cloutier
Cc:	Bhanu Pothugunta; Anil Kumar Prathipati; Colleen McCormack
Subject:	Re: Request to enable ports to generate TFA
Date:	Wednesday, October 10, 2018 8:10:23 AM

Dan,

Good morning. We are able to access our proxy server to send SMS and Email through AWS. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Oct 9, 2018, at 4:05 PM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> All servers should now have access to the destination you have requested. Please test and let me know the outcome.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Daniel J Cloutier
> **Sent:** Tuesday, October 9, 2018 11:24 AM
> **To:** 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
> **Cc:** Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
> **Subject:** RE: Request to enable ports to generate TFA
>
> Keval & Bhanu,
>
> The [redacted] servers already have access. I will request access for the dmz servers.
>
> Thanks,

Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both [redacted] ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: [redacted]
Public [redacted]
Ports [redacted]

Servers:

IP ADDRESS	SERVER
[redacted]	OLD UAT
[redacted]	OLD APP SER 1 & 2 Multiple Instances
[redacted]	OLD RPT
[redacted]	New App server
[redacted]	New UAT server
[redacted]	New Production Report server
[redacted]	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: John Penney
To: Colleen McCormack
Subject: RE: Statewide Checklist
Date: Tuesday, February 19, 2019 1:37:21 PM
Attachments: image001.png

Colleen,

I just downloaded the file.

Thanks,
John

JOHN PENNEY
Technical Support Specialist
NH Department of State
Phone: 603-271-8852
E-mail: John.Penney@sos.nh.gov

From: Colleen McCormack
Sent: Tuesday, February 19, 2019 10:58 AM
To: John Penney
Subject: Statewide Checklist

John,
The Statewide checklist ran on 02/12/2019. Did you save it?
It is running once a month from now on through April, until I update the election dates.
Let me know if you did save it.
Thanks

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: John Penney
To: Colleen McCormack
Subject: RE: Statewide Checklists
Date: Friday, September 21, 2018 8:05:18 AM
Attachments: image001.png

Colleen,

Do you know why checklist job ran twice this morning?

JOHN PENNEY
Technical Support Specialist
NH Department of State
Phone: 603-271-8852
E-mail: John.Penney@sos.nh.gov

From: Colleen McCormack
Sent: Tuesday, September 18, 2018 3:35 PM
To: John Penney
Subject: RE: Statewide Checklists

LOL

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: John Penney
Sent: Tuesday, September 18, 2018 3:33 PM
To: Colleen McCormack
Subject: RE: Statewide Checklists

Me neither…

JOHN PENNEY
Technical Support Specialist
NH Department of State
Phone: 603-271-8852
E-mail: John.Penney@sos.nh.gov

From: Colleen McCormack
Sent: Tuesday, September 18, 2018 3:32 PM
To: John Penney
Subject: RE: Statewide Checklists

I have not looked since last week.
I will look into it.
Thanks!

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: John Penney
Sent: Tuesday, September 18, 2018 3:30 PM
To: Colleen McCormack
Subject: RE: Statewide Checklists

Colleen,

I looks like the job hasn't run since last Friday. Is there something I'm missing?

JOHN PENNEY

Technical Support Specialist
NH Department of State
Phone: 603-271-8852
E-mail: John.Penney@sos.nh.gov

From: Colleen McCormack
Sent: Thursday, September 13, 2018 7:37 AM
To: John Penney
Subject: Statewide Checklists

John,

I have just rescheduled the statewide checklist to run daily as of tonight for the State General Election.

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta
To: Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: TFA - ElectioNet
Date: Monday, October 15, 2018 2:38:30 PM

Understood. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Monday, October 15, 2018 2:34 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: TFA - ElectioNet

Bhanu,
Thank you.
We are preparing for a Clerk Statewide conference.

I will not have time to test the TFA until after I come back from the conference.

The conference is October 23 – 26th.

I am off this Friday and Monday to NC to see my son.

I will try and have my staff start some testing as soon as possible.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Monday, October 15, 2018 2:26 PM
To: Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: FW: TFA - ElectioNet

Colleen,

As discussed, we have made following changes to UAT. Please review and let us know your comments. Thank You.

1. Maintain TFA:
    a. Code Expiry drop down should have up to 15 mins(3,5,10, 15).
    b. Verification expiry up to one hour(15,30,45,1).
    c. Remember devices reset days should have days(1,7,15,30,60,90).
2. Maintain Users -> Modify User should have option to Enable/Disable TFA.
3. Maintain Roles:
    a. If TFA is enabled to the role then do not allow to modify.
    a. If TFA is disabled, allow user to enable TFA.
4. Only State user can modify users Phone and Email.
5. Remove validation for address in “My Information Screen”.
6. Once Email/Phone verified, “Continue to Login” should redirect to get the TFA Text message screen.
7. Remember devices -> Browser version issue.
8. Remember devices screen should be displayed User level.
9. Enter TFA code -> By default cursor should focus on text box.
10. Disable double click on “Verify/Text me” buttons.
11. Label change TFA to 2FA.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack
To: Keval Patel
Cc: Bhanu Pothugunta; Sachin Shetty; Anil Kumar Prathipati
Subject: RE: Two Factor authentication
Date: Wednesday, October 10, 2018 9:13:44 AM

Sounds good to me.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Wednesday, October 10, 2018 8:38 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta; Sachin Shetty; Anil Kumar Prathipati
Subject: Re: Two Factor authentication

How about 1pm? If this work then we'll send you webex meeting. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Oct 10, 2018, at 8:17 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Yes I do...

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Wednesday, October 10, 2018 7:54 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta; Sachin Shetty; Anil Kumar Prathipati
Subject: Re: Two Factor authentication

Colleen,

Good morning. Do you have time today to see 2FA in UAT?

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Sep 27, 2018, at 11:02 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> I am available most of the day today until 4:00 PM.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State

State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Thursday, September 27, 2018 11:01 AM
To: Colleen McCormack; Bhanu Pothugunta
Cc: Sachin Shetty; Anil Kumar Prathipati
Subject: RE: Two Factor authentication

Colleen,

Please let me know when you are available to discuss this today. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, September 27, 2018 10:51 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Two Factor authentication

Bhanu,
I have documented some initial issues with TFA.
See the attached document.

Thank You,

Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Wednesday, September 26, 2018 6:49 PM
To: Colleen McCormack
Cc: Keval Patel; Sachin Shetty; Anil Kumar Prathipati
Subject: RE: Two Factor authentication

Colleen,

We have moved TFA module to UAT. We are getting connection issues for sending SMS and email. We will work with Dan tomorrow and update you. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Bhanu Pothugunta
Sent: Tuesday, September 25, 2018 8:39 PM
To: 'Colleen McCormack' <Colleen.McCormack@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Two Factor authentication

Colleen,

As discussed, we will move the Two Factor authentication code to UAT by

tomorrow. Also, please find the attached Two Factor authentication user manual for your reference.
We will setup a web ex meeting to go through the TFA process once we deployed in UAT. Please review and let us know if you have any questions.
Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From:	Bhanu Pothugunta
To:	Keval Patel; Colleen McCormack
Cc:	Sachin Shetty; Anil Kumar Prathipati
Subject:	RE: Two Factor authentication
Date:	Thursday, September 27, 2018 11:08:50 AM

Colleen,

Please connect to my webex. Following is the webex link. We will call you in 5 minutes. Thank You.

https://pcctg.webex.com/join/bhanu.pothugunta

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Keval Patel
Sent: Thursday, September 27, 2018 11:03 AM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Two Factor authentication

Ok. Call you soon. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, September 27, 2018 11:02 AM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Two Factor authentication

I am available most of the day today until 4:00 PM.

Thank You,
Colleen
Colleen E. McCormack
HAVA

Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Thursday, September 27, 2018 11:01 AM
To: Colleen McCormack; Bhanu Pothugunta
Cc: Sachin Shetty; Anil Kumar Prathipati
Subject: RE: Two Factor authentication

Colleen,

Please let me know when you are available to discuss this today. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Thursday, September 27, 2018 10:51 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Two Factor authentication

Bhanu,
I have documented some initial issues with TFA.
See the attached document.

Thank You,
Colleen
Colleen E. McCormack

HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Wednesday, September 26, 2018 6:49 PM
To: Colleen McCormack
Cc: Keval Patel; Sachin Shetty; Anil Kumar Prathipati
Subject: RE: Two Factor authentication

Colleen,

We have moved TFA module to UAT. We are getting connection issues for sending SMS and email. We will work with Dan tomorrow and update you. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Bhanu Pothugunta
Sent: Tuesday, September 25, 2018 8:39 PM
To: 'Colleen McCormack' <Colleen.McCormack@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Sachin Shetty <Sachin.Shetty@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Two Factor authentication

Colleen,

As discussed, we will move the Two Factor authentication code to UAT by tomorrow. Also, please find the attached Two Factor authentication user manual for your reference.
We will setup a web ex meeting to go through the TFA process once we deployed in UAT. Please review and let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta

O: 860.580.7687
M: 860.752.3834

From: Amy Cohen
To: Amy Cohen
Subject: Re: Update, 5/20
Date: Tuesday, May 21, 2019 3:07:16 PM

The House Admin hearing got pushed to 2:45pm ET and hasn't started yet. If the link on their website isn't working, you can also stream it on CSPAN.

In addition, the National Security Subcommittee hearing should be livestreamed tomorrow.

Amy

From: Amy Cohen <acohen@nased.org>
Date: Monday, May 20, 2019 at 12:21 PM
To: Amy Cohen <acohen@nased.org>
Subject: Update, 5/20

Happy Monday!

- Attached please find a document provided by DHS on some recent YARA rules, which are characteristics for identifying malware. While this will mostly not be meaningful to policy staff, please make sure your technical staff sees this and acts on it.
- Reminder that the EAC's last public hearing is this afternoon at 1:30pm ET. Livestream available here. Witnesses:
    - Iowa Secretary of State Paul Pate
    - Traci Mapps, SLI Compliance
    - Jack Cobb, Pro V&V
    - Joseph Lorenzo Hall, Center for Democracy and Technology
- The House Administration Committee will hold an EAC Oversight hearing tomorrow at 2:00pm that will be livestreamed. All four EAC commissioners will be in attendance. Testimony available here.
- The House Government Oversight National Security Subcommittee will hold a hearing on "Securing U.S. Election Infrastructure and Protecting Political Discourse" on Wednesday, May 22 at 2pm ET. I don't know if it will be livestreamed, but if it is, I will send it around when I have it. Witnesses will be:
    - Panel 1
        - Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS
        - Adam Hickey, Deputy Assistance Attorney General, National Security Division, US Department of Justice
        - Christy McCormick, Chair, EAC
        - Department of Defense (invited)
    - Panel 2

- Bill Galvin, Massachusetts Secretary of State
- Richard Salgado, Director of Law Enforcement and Information Security, Google
- Nathanial Gleicher, Head of Cybersecurity Policy, Facebook
- Kevin Kane, Public Policy Manager, Twitter

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From:	Daniel J Cloutier
To:	Keval Patel
Cc:	Anthony Stevens; Colleen McCormack; Bhanu Pothugunta; Anil Kumar Prathipati; Ganesh Veerabathiran
Subject:	RE: Using Amazon for 2-factor authentication
Date:	Thursday, January 31, 2019 9:34:20 AM

The question is coming up because we have ProofPoint and it has been quarantine the messages. We have found a way to allow the messages through so nothing has to change at this time.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Thursday, January 31, 2019 8:58 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>
Subject: RE: Using Amazon for 2-factor authentication

Amazon service we use for email and SMS both. My experienced with other states AWS response time is very reliable. We can use SOS email server if you have any concerns but we still need to use AWS service for SMS. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, January 31, 2019 8:37 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Using Amazon for 2-factor authentication

Keval,

Why are we using an Amazon service to send the 2FA messages instead of using our own SOS email server?

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

REQUEST FOR APPLICATIONS

Policy Academy on Election Cybersecurity

IMPORTANT INFORMATION

Purpose: To maximize public confidence in elections by reducing technical risks to election systems and improving coordination between election officials and state cybersecurity leaders in the executive branch.

Opportunities Provided: Teams from five (5) competitively selected states will convene stakeholder workshops within their states to identify, refine, and/or implement promising practices in cybersecurity operations and communications directly related to elections.

Proposals Due:	8:00 PM ET, May 10, 2019
Informational Calls:	3:00 PM ET, April 5, 2019 2:00 PM ET, April 18, 2019 Conference Number: 888-858-6021 Conference Code: 202-624-5356
Selection Announcement:	Week of May 27, 2019
Project Period:	June 1, 2019 – December 1, 2019
Eligibility:	All eligible states, commonwealths, and territories.
NGA Contacts:	Maggie Brunner, Program Director, Cybersecurity and Communications, Homeland Security & Public Safety Division (202) 624-5364 or mbrunner@nga.org David Forscey, Senior Policy Analyst, Homeland Security & Public Safety Division (202) 624-5356 or dforscey@nga.org

PURPOSE

Election cybersecurity is a complex, long-term challenge that demands coordination across state and local governments. The National Governors Association Center for Best Practices (NGA Center)—in conjunction with technical support from the University of Southern California (USC)—is launching the *Policy Academy on Election Cybersecurity*, designed to facilitate intrastate dialogue and planning between election officials, governors' offices, and state cabinet agencies. This project will offer technical assistance to five states that have committed to improving intrastate coordination around election cybersecurity practices, policy, and planning. Combining expertise in state policy and technical research, the NGA Center will help interested states enhance interagency communication and cooperation, promote engagement by governors' offices, and

Application Checklist on Final Page

facilitate the development of statewide response plans for attacks on election infrastructure. Technical assistance offerings include facilitated strategic planning, policy design and development, state comparative analysis, document drafting, access to subject matter experts, and general capacity building.

Supporting organizations for the Policy Academy on Election Cybersecurity *include the National Association of State Election Directors and the National Association of Secretaries of State. Funding is provided by the Democracy Fund.*

BACKGROUND

Election officials have worked diligently against malicious attempts to undermine public trust in elections. Well before the 2016 elections, these efforts included important steps to address security vulnerabilities in voting systems, election management systems, and the procedures that rely on those systems.

Since 2016, the elections community has devoted unprecedented time, attention, and funding into cybersecurity controls designed to reduce risk. Driving these concerted efforts is evidence that foreign governments possess the means and intent to influence elections in the United States.

Notwithstanding geopolitics, other developments further underscore the need to prioritize election cybersecurity. First, in recent years, highly sophisticated hacking tools have become widely available, empowering novice attackers. Second, media reports have increased public concern about the security of elections and even highlighted opportunities for election interference. Third, increased public reliance on social networks for information magnifies the risks posed by isolated security events. For example, a single incident, real or perceived, affecting one voting or election system in one jurisdiction—reported by news media and amplified through social media—could undermine public confidence in broader election outcomes. In short, election practitioners confront a long-term struggle against a diverse set of potential attackers, who are increasingly capable, with a range of motivations, and who cannot all be deterred with the same tools.

Addressing this threat demands a whole-of-government approach that integrates all relevant cybersecurity resources and planning. This requires coordination across independent agencies. In many states, elections are managed by an independently elected constitutional officer who does not report to the governor. Yet significant cybersecurity expertise and resources can be found in departments and agencies subordinate to the governor. State information technology, homeland security, and public safety departments have expertise and capabilities that can boost the capacity of election officials to defend voting systems and election systems. Many National Guard cyber units comprise experts who work full-time in world-class technology companies. In dozens of states, cybersecurity leaders under the governor are collaborating through formal and informal governance bodies to write statewide cybersecurity strategies and disruption response plans that will guide cybersecurity investment and assistance.

A series of obstacles are limiting coordination between the election community and governors' cybersecurity leaders. Although the 2016 elections advanced a dialogue between election officials and governors' advisors, decades of siloed operations have deprived all stakeholders of the personal relationships and mutual understanding that are critical for long-term collaboration. Election officials are often left out of statewide strategies and plans. Election offices seeking help from the National Guard may lack support from the governors' office to request Guard resources. Governors' offices and state cabinet leaders may not always know what election officials need, from funding and technical assistance to coordinated public messaging.

POLICY ACADEMY DESCRIPTION

In recognition of the above challenges, the NGA Center, in a partnership with the University of Southern California, is launching the *Policy Academy on Election Cybersecurity*. This initiative is designed to help states maximize public confidence by fostering long-term coordination between election officials, governors' offices, and state cybersecurity leaders.

An NGA policy academy is a highly collaborative, team-based process for helping a select number of states develop and implement action plans that address complex public policy challenges. Participating states receive guidance and technical assistance (e.g., facilitated workshops, policy research, written products) from NGA Center staff and, as appropriate, access to subject matter experts from the private sector, research organizations, academia, and the federal government. A policy academy provides a forcing mechanism that focuses the time and attention of stakeholder groups that can prove difficult to convene under normal circumstances. The strategies and policies developed by participating states are intended to catalyze wider adoption of promising practices across the United States. The *Policy Academy on Election Cybersecurity* will benefit from direct research support provided by staff and faculty from the University of Southern California. ***Note: This project is not an academic study, and no state-specific findings or conclusions will be published or otherwise shared or discussed publicly without the express consent of participating states and other relevant stakeholders.***

Key Benefits

The primary activities of the *Policy Academy on Election Cybersecurity* include (a) technical assistance provided by NGA Center staff and appropriate subject matter experts; (b) a two-day multidisciplinary, in-state workshop to convene election officials and state cybersecurity leaders to create action plans; and (c) limited funding to cover travel costs for stakeholders. These activities will support goals that states choose to prioritize. Examples of appropriate state goals include:

- Integrating the needs of election officials into statewide strategies and investment plans;
- Engaging new gubernatorial administrations and building support for past and future election cybersecurity initiatives;
- Identifying and/or communicating election cybersecurity needs, corresponding budgets, and legislative strategies;
- Creating election cybersecurity priorities, policies, and plans for National Guard units;
- Leveraging all existing state, federal and/or local resources to scale training and assistance for local election offices (e.g., shared services contracts);
- Creating a statewide communications strategy that coordinates election cybersecurity messaging across relevant state and local offices;
- Integrating election offices with state fusion centers or security operations centers, or establishing a dedicated center for election cybersecurity activities;
- Identifying gaps in state law and potential solutions;
- Facilitating conversations with critical infrastructure owners and operators (e.g., internet service providers or utilities).

State Team Responsibilities

The Policy Academy will require preparation from state attendees before the in-state workshop, active team participation throughout the policy academy process, and a strong commitment to implementing action plans. Specifically, participating states are required to:

- *Participate in scheduled conference calls.* Following state selection, the NGA Center will host conference calls with participating states to orient them to the Policy Academy and outline next steps, including policy academy preparatory work and meetings, available technical assistance and resources from NGA Center staff and other experts, and site visits by NGA Center staff. Monthly conference calls will maintain coordination until the in-state workshop. Conference calls may continue on an as-needed basis for states who request additional virtual technical assistance following the workshop.
- *Develop state needs assessment and gap analysis.* Through initial conferences calls and other preparatory work, the NGA Center will complete a confidential gap analysis and needs assessment for each state. The gap analysis and needs assessment will provide team members with a better understanding of their state's challenges and serve as a baseline for evaluating outcomes of the policy academy.
- *Convene an in-state workshop.* The in-state workshop provides the core benefit of the Policy Academy process. Staff from the NGA Center will conduct a two-day visit in each state to help teams identify and/or implement action plans to achieve the objectives outlined in the Policy Academy application. Active participation by the entire Policy Academy team is required.
- *Complete evaluation survey and lessons learned report.* After the Policy Academy, participating states will be asked to complete a survey for the NGA Center on the work they accomplished during the project. State responses will be used for evaluation purposes and, with the state's consent, will be included in a public report on the lessons learned during the Policy Academy, to be disseminated to all other states and territories.

POLICY ACADEMY APPLICATION PROCESS

(SEE APPLICATION CHECKLIST ON LAST PAGE)

Step 1: Secure Commitment from the Governor and Chief Election Official(s)

The goal of this Policy Academy is to improve intrastate coordination between governors' offices, state cabinet agencies, and election offices. Interested state teams should secure approval from the governor and the chief election official of the same state. Each team will be asked to submit a joint letter or separate letters of commitment from the governor and chief election official. (See Step 3.)

Step 2: Identify a Policy Academy Team

Each interested state should assemble a high-level multidisciplinary "core" team of state representatives, plus a larger, more comprehensive team. The core team will (a) manage the full team; (b) prioritize state objectives; and (c) lead coordination with the NGA Center and other relevant support organizations.

Team leads: The core team will be led by two state officials, one selected by the governor's office, and one selected by the chief state election official(s) (or by the designee of the chief state election official).

Application Checklist on Final Page

Core team: The team leads will designate the rest of the core team, comprising a mix of relevant representatives from each respective branch of government. The core team must include a minimum of six (6) state officials, including the team leads; each state is free to determine the appropriate size of its core team beyond the minimum. Two possible examples of core teams are:

- Example 1: Adjutant General, statewide Chief Information Officer, statewide Homeland Security Advisor, Secretary of State, Election Director, and Chief Information Officer for the statewide election office.
- Example 2: Head of the Department of Motor Vehicles, statewide Chief Information Security Officer, Commissioner of Public Safety, two county Election Directors, and the statewide Elections Commissioner.

Full team: The core team will designate a larger team that can include not only state officials, but also non-state and local actors, such as local election officials, academic advisors, nonprofit representatives, and others. *The full team does not need to be described in the written application.*

Step 3: Draft the Application Narrative. Formal applications to participate in the Policy Academy cannot exceed six (6) pages and must include:

(1) *Letter(s) of application from the governor and the chief election official:* The letter or letters of application, co-signed by the governor and chief election official (or, if using separate letters, signed by each), should briefly articulate the state's interest in and desired outcomes related to this project, and how those outcomes fit within the state's commitment to election security. The letter(s) must designate the two team leads who will direct the team's efforts with the NGA Center. The letter(s) will *not* count against the six-page limit.

(2) *Proposal narrative:* The proposal narrative should not exceed six-pages single-spaced, 11-point font, 1" margins. **Please see the final page of this document for evaluation criteria that offer a guide for narrative content**.

Step 4: Submit the Application. All proposals must be received by **5:00 PM PST on May 10, 2019**. Only one application per state will be considered, and it must be transmitted by a state employee. Prior to submission, please assemble the proposal materials into a single PDF document. **Please email the proposal to Maggie Brunner at mbrunner@nga.org.** NGA will confirm receipt within one business day.

POLICY ACADEMY TIMELINE

The following is a tentative schedule for the academy:

3:00 PM ET, April 5, 2019 Number: 888-858-6021 Code: 202-624-5356	**1st Bidders' Call** The NGA Center will host an optional conference call for all interested states to answer questions about the Request for Application (RFA) process, proposal content, submission requirements, or other issues.
2:00 PM ET, April 18, 2019 Number: 888-858-6021 Code: 202-624-5356	**2nd Bidders' Call**

Application Checklist on Final Page

	The NGA Center will host an optional conference call for all interested states to answer questions about the RFA process, proposal content, submission requirements, or other issues.
5:00 PM PST, May 10, 2019	**Proposals Due**
Week of May 27, 2019	**State Selection Announcement** The NGA Center will notify states of their application status and issue a press release announcing winning states.
June 2019 – December 2019	**In-State Workshops** Objectives: • Engage state team in planning process • Refine initial recommendations • Develop strategic action plan for implementing recommendations
Ongoing	Monthly conference calls and webinars with Policy Academy staff and other participating states.

SELECTION CRITERIA **(Total points possible = 100 pts)**

Note: States can use these criteria in drafting the narrative portion of their application.

Category	Description	Value
Description of the Problem	• Applicants should describe current efforts to secure election and voting infrastructure at the state and local levels. • Applicants should explain limitations of the state's current approach that may be relevant.	20 points
Anticipated Benefits and Potential Outcomes	• Applicants should explain how improving coordination between election offices and other state cybersecurity offices will help the state address identified challenges and improve their overall efforts to secure elections. They should articulate a clear "business case" for how proposed changes will help them achieve state goals. • Applicants must demonstrate that the state is poised to make significant progress toward improving their statewide efforts to secure election infrastructure. For example, is there buy-in from key political leaders, agency leadership, local government, and communities? If not, will the Policy Academy help to solve that? • Applicants should identify specific outcomes they hope to achieve by the end of the Policy Academy. *Applicants should focus on activities that support election cybersecurity. This Policy Academy will not focus on information operations.*	30 points
Obstacles to Implementing Solutions	***This section does not count toward the six-page limit.***	20 points

Application Checklist on Final Page

	• Applicants should identify any potential obstacles that could derail development or implementation of their goals. Further, they should explain how they might address those challenges. *For states that are undergoing a gubernatorial or chief election official transition, please address how you will pursue completion of Policy Academy goals and activities through that transition.*	
Evaluation Plan	• Applicants must identify a plan that ties goals and objectives to tangible metrics. • Describe what those metrics are and how they would be measured. ***This section does not count toward the six-page limit.***	10 points

Team Composition and Member Roles	***This section does not count toward the six-page limit.***
	
	• **Team Leads**: The governor and chief election official must each designate a separate representative from their branch to co-lead the state's Policy Academy project.
	• **Core Team**: Each state must assemble a multi-disciplinary "core" team comprising of a minimum of six (6) state leaders (including the team leads) with demonstrated equities in elections, cybersecurity, homeland security, and/or emergency preparedness. Applicants should briefly discuss the rationale behind the core team composition and the roles and responsibilities each member will take on in support of achieving team objectives.
	  ○ Please provide each core team member's name, title, work address, phone, and e-mail address.
	  ○ *Note: resumes or curriculum vitae are not required.*
	• **Full Team:** States can identify additional members of the full team, above and beyond the core team. This can be a much broader and more diverse group, and can include state, local, and non-governmental partners, to consult with during the Policy Academy and to convene during the state's two-day workshop.
	  ○ Note: For purposes of the full team members, simply listing agencies/affiliations, rather than specific individuals, is sufficient.
	
	This section does not count toward the six-page limit.
		20 points

Disclaimers

This request for application is not binding on the NGA Center, nor does it constitute a contractual offer. Without limiting the foregoing, the NGA Center reserves the right, in its sole discretion, to reject any or all applications; to modify, supplement, or cancel the RFA; to waive any deviation from the RFA; to negotiate regarding any application; and to negotiate final terms and conditions that may differ from those stated in the RFA. Under no circumstances shall NGA Center be liable for any costs incurred by any person in connection with the preparation and submission of a response to this RFA.

Application Checklist on Final Page

Policy Academy on Election Cybersecurity
Application Checklist

Application Process

- ☐ Consult with Governor's Office and Chief Election Official Regarding Application Process
- ☐ Identify Team Leads
- ☐ Identify Core Team
- ☐ Prepare Narrative Description (maximum of six (6) pages single-spaced)
- ☐ Email Application in PDF Format to Maggie Brunner at mbrunner@nga.org **before 5:00 PM PST on May 10, 2019**.

Application Contents

- ☐ Letter(s) of Application from Governor and Chief Election Official
- ☐ Narrative Description (Maximum length of six (6) pages, single-spaced)
  - Description of the Problem
  - Anticipated Benefits and Potential Outcomes
  - Obstacles to Implementing Solutions
  - Evaluation Plan (does not count toward the page limit)
  - Team Composition (does not count toward the page limit)
    - Team Leads
    - Core Team
    - Full Team (optional—members of the full team can be identified after the Policy Academy application has been submitted)

REQUEST FOR APPLICATIONS

Policy Academy on Election Cybersecurity

IMPORTANT INFORMATION

Purpose: To maximize public confidence in elections by reducing technical risks to election systems and improving coordination between election officials and state cybersecurity leaders in the executive branch.

Opportunities Provided: Teams from five (5) competitively selected states will convene stakeholder workshops within their states to identify, refine, and/or implement promising practices in cybersecurity operations and communications directly related to elections.

Proposals Due:	5:00 PM PST, May 10, 2019
Informational Calls:	2:00 PM ET, April 10, 2019 2:00 PM ET, April 18, 2019 Conference Number: 888-858-6021 Conference Code: 202-624-5356
Selection Announcement:	Week of May 27, 2019
Project Period:	June 1, 2019 – December 1, 2019
Eligibility:	All eligible states, commonwealths, and territories.
NGA Contacts:	Maggie Brunner, Program Director, Cybersecurity and Communications, Homeland Security & Public Safety Division (202) 624-5364 or mbrunner@nga.org David Forscey, Senior Policy Analyst, Homeland Security & Public Safety Division (202) 624-5356 or dforscey@nga.org

PURPOSE

Election cybersecurity is a complex, long-term challenge that demands coordination across state and local government. The National Governors Association Center for Best Practices (NGA Center)—in conjunction with technical support from the University of Southern California (USC)—is launching the *Policy Academy on Election Cybersecurity* to facilitate intrastate dialogue and planning between election officials, governors' offices, and state cabinet agencies by providing technical assistance to five states that have committed to improving intrastate coordination around election cybersecurity practices, policy, and planning. Combining expertise in state policy and technical research, the NGA Center will help interested states enhance interagency communication and cooperation, promote engagement by governors' offices, and facilitate the development of

Application Checklist on Final Page

statewide response plans for attacks on election infrastructure. Technical assistance offerings include facilitated strategic planning, policy design and development, state comparative analysis, document drafting, access to subject matter experts, and general capacity building.

Supporting organizations for the Policy Academy on Election Cybersecurity include the National Association of State Election Directors and the National Association of Secretaries of State. Funding is provided by the Democracy Fund.

BACKGROUND

Election officials have always worked diligently against malicious attempts to undermine public trust in elections. Well before the 2016 elections, these efforts included important steps to address security vulnerabilities in voting systems, election management systems, and the procedures that rely on those systems.

In the past two years, the elections community has poured unprecedented time, attention, and funding into cybersecurity controls designed to reduce risk. Driving these concerted efforts is evidence that foreign governments possess the means and intention to influence elections in the United States.

Notwithstanding geopolitics, other developments further underscore the need to prioritize election cybersecurity. First, in recent years, highly sophisticated hacking tools have become widely available, empowering novice attackers. Second, media reports have increased public concern about the security of elections and even highlighted opportunities for election interference. Third, increased public reliance on social networks for information magnifies the risks posed by isolated security events. For example, a single incident, real or perceived, affecting one voting or election system in one jurisdiction—reported by news media and amplified through social media (or vice versa)—could undermine public confidence in broader election outcomes. In short, election practitioners confront a long-term struggle against a diverse set of potential attackers, who are increasingly capable, with a range of motivations, and who cannot all be deterred with the same tools.

Addressing this threat demands a whole-of-government approach that integrates all relevant cybersecurity resources and planning. This requires coordination across independent agencies. In many states, elections are managed an independently elected constitutional officer who does not report to the governor. Yet significant cybersecurity expertise and resources can be found in departments and agencies subordinate to the governor. State information technology, homeland security, and public safety departments have established important resources that can boost the capacity of election officials to defend voting systems and election systems. Many National Guard cyber units comprise experts who work full-time in world-class technology companies. In dozens of states, cybersecurity leaders under the governor are collaborating through formal and informal governance bodies to write statewide cybersecurity strategies and disruption response plans that will guide cybersecurity investment and assistance.

A series of obstacles are limiting coordination between the election community and governors' cybersecurity leaders. Although the 2016 elections precipitated a dialogue between election officials and governors' advisors, decades of siloed operations have deprived all stakeholders of the personal relationships and mutual understanding that are critical for long-term collaboration. Election officials are often left out of statewide strategies and plans. Election offices seeking help from the National Guard may lack support from the governors' office to request Guard resources. Governors' offices and state cabinet leaders may not always know what election officials need, from funding and technical assistance to coordinated public messaging.

Application Checklist on Final Page

POLICY ACADEMY DESCRIPTION

In recognition of the above challenges, the NGA Center, in a partnership with the University of Southern California, is launching the *Policy Academy on Election Cybersecurity*, an initiative designed to help states maximize public confidence by fostering long-term coordination between election officials, governors' offices, and state cybersecurity leaders.

An NGA policy academy is a highly collaborative, team-based process for helping a select number of states develop and implement action plans that address complex public policy challenges. Participating states receive guidance and technical assistance (e.g., facilitated workshops, policy research, written products) from NGA Center staff and, as appropriate, access to subject matter experts from the private sector, research organizations, academia, and the federal government. A Policy Academy provides a forcing mechanism that focuses the time and attention of stakeholder groups that can prove difficult to convene under normal circumstances. The strategies and policies developed by participating states are intended to catalyze wider adoption of promising practices across the United States. The *Policy Academy on Election Cybersecurity* will benefit from direct research support provided by staff and faculty from the University of Southern California. ***Note: This project is not an academic study, and no findings or conclusions will be published without the express consent of participating states.***

Key Benefits

The primary benefits of the *Policy Academy on Election Cybersecurity* include (a) technical assistance provided by NGA Center staff and appropriate subject matter experts; (b) a two-day multidisciplinary, in-state workshop to convene election officials and state cybersecurity leaders to create action plans; and (c) limited funding to cover travel costs for stakeholders. These activities will support goals that states choose to prioritize. Examples of appropriate state goals include:

- Integrating the needs of election officials into statewide strategies and investment plans;
- Engaging new gubernatorial administrations and building support for past and future election cybersecurity initiatives;
- Identifying and/or communicating election cybersecurity needs, corresponding budgets, and legislative strategies;
- Creating election cybersecurity priorities, policies, and plans for National Guard units;
- Leveraging all existing state, federal and/or local resources to scale training and assistance for local election offices (e.g., shared services contracts);
- Creating a statewide communications strategy that coordinates election cybersecurity messaging across all relevant state and local offices;
- Integrating election offices with state fusion centers or security operations centers, or establishing a dedicated center for election cybersecurity activities;
- Identifying gaps in state law and potential solutions;
- Facilitating conversations with critical infrastructure owners and operators (e.g., internet service providers or utilities).

State Team Responsibilities

The Policy Academy will require preparation from state attendees before the in-state workshop, active team participation throughout the policy academy process, and a strong commitment to implementing action plans. Specifically, participating states are required to:

- *Participate in scheduled conference calls.* Following state selection, the NGA Center will host a conference call with participating states to orient them to the Policy Academy and outline next steps, including policy academy preparatory work and meetings, available technical assistance and resources from NGA Center staff and other experts, and site visits by NGA Center staff. Monthly conference calls will maintain coordination until the in-state workshop.
- *Develop state needs assessment and gap analysis.* Through initial conferences calls and other preparatory work, the NGA Center will complete a confidential gap analysis and needs assessment for each state. The gap analysis and needs assessment will provide team members with a better understanding of their state's challenges and serve as a baseline for evaluating outcomes of the policy academy.
- *Convene an in-state workshop.* The in-state workshop provides the core benefit of the Policy Academy process. Staff from the NGA Center will conduct a two-day visit in each state to help teams identify and/or implement action plans to achieve the objectives outlined in the Policy Academy application. Active participation by the entire Policy Academy team is required.
- *Complete evaluation survey and lessons learned report.* After the Policy Academy, participating states will be asked to complete a brief survey for the NGA Center on the work they accomplished during the project. State responses will be used for evaluation purposes and, with the state's consent, will be included in a public report on the lessons learned during the Policy Academy, to be disseminated to all other states and territories.

POLICY ACADEMY APPLICATION PROCESS

(SEE APPLICATOIN CHECKLIST ON LAST PAGE)

Step 1: Secure Commitment from the Governor and Chief Election Official(s)

The goal of this Policy Academy is to improve intrastate coordination between governors' offices, state cabinet agencies, and election offices. Interested state teams should secure approval from the governor and the chief election official(s) of the same state. Each team will be asked to submit a joint letter or separate letters of commitment from the governor and chief election official. (See Step 3.)

Step 2: Identify a Policy Academy Team

Each interested state should assemble a high-level multidisciplinary "core" team of state representatives, plus a larger, more comprehensive team. The core team will (a) manage the full team; (b) prioritize state objectives; and (c) lead coordination with the NGA Center and other relevant support organizations.

Team leads: The core team will be led by two state officials, one selected by the governor's office, and one selected by the chief state election official(s) (or designee of the chief state election official).

Core team: The team leads will designate the rest of the core team, comprising a mix of relevant representatives from each respective branch of government. The core team must

Application Checklist on Final Page

include a minimum of six (6) state leaders, including the team leads; each state is free to determine the appropriate size of its core team beyond the minimum. For example, a core team might include the following leaders: Adjutant General, statewide Chief Information Officer, statewide Homeland Security Advisor, Secretary of State, Election Director, and Chief Information Officer for the statewide election office.

Full team: The core team will designate a larger team that can include not only state officials, but also non-state and local actors, such as local election officials, academic advisors, nonprofit representatives, and others. *The full team does not need to be described in the written application.*

Step 3: Draft the Application Narrative. Formal applications to participate in the Policy Academy cannot exceed six (6) pages and must include:

(1) *Letter(s) of application from the governor and chief election official(s):* The letter or letters of application, co-signed by the governor and chief election official(s) (or, if using separate letters, signed by each), should briefly articulate the state's interest in and desired outcomes related to this project, and how those outcomes fit within the state's commitment to election security. The letter(s) must designate the two team leads who will direct the team's efforts with the NGA Center. The application letter(s) will *not* count against the six-page limit.

(2) *Proposal narrative:* The proposal narrative should not exceed six-pages single-spaced, 11-point font, 1" margins. **Please see the final page of this document for evaluation criteria that offer a guide for narrative content**.

Step 4: Submit the Application. All proposals must be received by **5:00 PM PST on May 10, 2019**. Only one application per state will be considered, and it must be transmitted by a state employee. Prior to submission, please assemble the proposal materials into a single PDF document. **Please email the proposal to Maggie Brunner at mbrunner@nga.org.** NGA will confirm receipt within one business day.

POLICY ACADEMY TIMELINE

The following is a tentative schedule for the academy:

2:00 PM ET, April 10, 2019 Number: 888-858-6021 Code: 202-624-5356	**1st Bidders' Call** The NGA Center will host an optional conference call for all interested states to answer questions about the RFA process, proposal content, submission requirements, or other issues.
2:00 PM ET, April 18, 2019 Number: 888-858-6021 Code: 202-624-5356	**2nd Bidders' Call** The NGA Center will host an optional conference call for all interested states to answer questions about the RFA process, proposal content, submission requirements, or other issues.
5:00 PM PST, May 10, 2019	**Proposals Due**
Week of May 27, 2019	**State Selection Announcement** The NGA Center will notify states of their application status and issue a press release announcing winning states.
June 2019 – December 2019	**In-State Workshops** Objectives: • Engage state team in planning process

Application Checklist on Final Page

	• Refine initial recommendations • Develop strategic action plan for implementing recommendations
Ongoing	Monthly conference calls and webinars with Policy Academy staff and other participating states.

SELECTION CRITERIA **(Total points possible = 100 pts)**

Note: States can use these criteria in drafting the narrative portion of their application.

Category	Description	Value
Description of the Problem	• Applicants should describe current efforts to secure election and voting infrastructure at the state and local levels. • Applicants should explain limitations of the state's current approach that may be relevant.	20 points
Anticipated Benefits and Potential Outcomes	• Applicants should explain how improving coordination between election offices and other state cybersecurity offices will help the state address identified challenges and improve their overall efforts to secure elections. They should articulate a clear "business case" for how proposed changes will help them achieve state goals. • Applicants must demonstrate that the state is poised to make significant progress toward improving their statewide efforts to secure election infrastructure. For example, is there buy-in from key political leaders, agency leadership, local government, and communities? If not, will the Policy Academy help to solve that? • Applicants should identify specific outcomes they hope to achieve by the end of the policy academy. *Applicants should focus on activities that support election cybersecurity. This Policy Academy will not focus on information operations.*	30 points
Challenges to Implementing Solutions	• Applicants should identify any potential challenges that could derail development or implementation of their goals. Further, they should explain how they might address those challenges. *For states that are undergoing a gubernatorial or chief election official transition, please address how you will pursue completion of policy academy goals and activities through that transition.*	20 points
Evaluation Plan	• Applicants must identify a plan that ties goals and objectives to tangible metrics. • Describe what those metrics are and how they would be measured.	10 points

Application Checklist on Final Page

	This section does <u>not</u> count toward the six-page limit.	
Team Composition and Member Roles	• **Team Leads**: The governor and chief election official must each designate a separate representative from their branch to co-lead the state's Policy Academy project. • **Core Team**: Each state must assemble a multi-disciplinary "core" team comprising of a minimum of six (6) state leaders (including the team leads) with demonstrated equities in elections, cybersecurity, homeland security, and/or emergency preparedness. Applicants should briefly discuss the rationale behind the core team composition and the roles and responsibilities each member will take on in support of achieving team objectives. o Please provide each core team member's name, title, work address, phone, and e-mail address. o *Note: resumes or curriculum vitae are <u>not</u> required.* • **Full Team:** States should identify additional members of the full team, above and beyond the core team. This can be a much broader and more diverse group, and can include state, local, and non-governmental partners, to consult with during the Policy Academy and to convene during the state's two-day workshop. o Note: for purposes of the full team members, simply listing agencies/affiliations, rather than specific individuals, is sufficient. *This section does <u>not</u> count toward the six-page limit.*	20 points

Disclaimers

This request for application is not binding on the NGA Center, nor does it constitute a contractual offer. Without limiting the foregoing, the NGA Center reserves the right, in its sole discretion, to reject any or all applications; to modify, supplement, or cancel the RFA; to waive any deviation from the RFA; to negotiate regarding any application; and to negotiate final terms and conditions that may differ from those stated in the RFA. Under no circumstances shall NGA Center be liable for any costs incurred by any person in connection with the preparation and submission of a response to this RFA.

Policy Academy on Election Cybersecurity
Application Checklist

Application Process

- ☐ Obtain Permission to Apply from Governor and Chief Election Official(s)
- ☐ Identify Team Leads
- ☐ Identify Core Team
- ☐ Prepare Narrative Description (maximum of six (6) pages single-spaced)
- ☐ Email Application to Maggie Brunner at mbrunner@nga.org **before 5:00 PM PST on May 10, 2019**.

Application Contents

- ☐ Letter(s) of Application from Governor and Chief Election Official(s)
- ☐ Narrative Description (Maximum length of six (6) pages, single-spaced)
  - Description of the Problem
  - Anticipated Benefits and Potential Outcomes
  - Challenges to Implementing Solutions
  - Evaluation Plan
  - Team Composition
    - Team Leads
    - Core Team
    - Full Team (optional—members of the full team can be identified after the Policy Academy application has been submitted)

Application Checklist on Final Page

Election Officials Regional Forum

★ ★ ★ ★ ★ ★ ★ ★ ★ ★

June 11-12, 2019

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Region I and the President of the National Association of Secretaries of State / Vermont Secretary of State invites you to participate in a State Election Officials Regional Forum on **June 11th and 12th, 2019** at the University of New Hampshire – Durham NH.

Since 2016, CISA has led a voluntary partnership of federal government and election officials to safeguard our election system. In order to further enhance this coordinated approach, this forum will provide you the opportunity to:

- Share best practices/lessons learned from the 2018 election cycle with fellow New England elections officials and federal partners;
- Receive information-sharing capabilities briefings from federal partners DHS/CISA, DHS Intelligence & Analysis, U.S. Secret Service, and the Federal Bureau of Investigation;
- Discuss the state of New England's technological capabilities and priorities in the run-up to 2020; and
- Conduct targeted break-out sessions to assess potential critical infrastructure threats and resource gaps.

This forum is designed to primarily benefit the Secretary of State, Deputy Secretary, Chief of Staff, Elections Director, Elections Administrator, State CISO, Information Technology Manager, and Homeland Security Advisor. We hope you will join us for this unique opportunity to work collaboratively with your state and federal partners to address the evolving challenges facing our election infrastructure.

Please RSVP to IPRegion1@hq.dhs.gov by May 10, 2019. If you have any questions, feel free to email us at IPRegion1@hq.dhs.gov or call Tracy Shawyer at 202-870-7698.

We look forward to engaging with you!

116TH CONGRESS
1ST SESSION

S. _____

To provide grants to support continuing education in election administration or cybersecurity for election officials and employees.

IN THE SENATE OF THE UNITED STATES

_____

_____ introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide grants to support continuing education in election administration or cybersecurity for election officials and employees.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Elections Require Investment in Vigilant Staff Act" or the "SERVIS Act".

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) free and fair elections are central to our democracy;

(2) protecting our elections from foreign adversaries is a national security priority;

(3) the States conduct elections and it is important to maintain State leadership in election administration;

(4) the States deserve Federal support to secure our elections from interference by foreign nations; and

(5) election security in the United States will benefit from continued education and investment in the individuals that administer our elections.

SEC. 3. SUPPORTING CONTINUING EDUCATION FOR ELECTION OFFICIALS AND EMPLOYEES.

(a) PROGRAM AUTHORITY AND METHOD OF DISTRIBUTION.—The Election Assistance Commission (in this section referred to as the "Commission") shall establish a program under which the Commission pays to each eligible institution such sums as may be necessary to pay to each eligible certificate program enrollee (as defined in subsection (b)) for each academic year during which that enrollee is enrolled in an accredited certificate program in election administration or cybersecurity in the amount for which that enrollee is eligible, as determined pursuant to subsection (c). Not less than 85 percent of such sums shall be advanced to eligible institutions prior to the start of

each payment period and shall be based upon an amount requested by the institution as needed to pay eligible certificate program enrollees until such time as the Commission determines an alternative payment system that provides payments to institutions in an accurate and timely manner, except that this sentence shall not be construed to limit the authority of the Commission to place an institution on a reimbursement system of payment.

(b) ELIGIBLE CERTIFICATE PROGRAM ENROLLEE.—In this section, the term "eligible certificate program enrollee" means an individual who—

(1) is a State or local election official, an employee of a State or local election official, or an employee of the Commission;

(2) certifies to the Commission their enrollment in an accredited certificate program in election administration or cybersecurity; and

(3) submits to the Commission—

(A) a receipt or other verification determined appropriate by the Commission of the tuition amount for such certificate program; and

(B) an application at such time, in such manner, and containing such information as the Commission may require.

(c) AMOUNT OF GRANTS.—The amount of a grant for an eligible certificate program enrollee under this section for a year shall be an amount equal to 75 percent of the tuition amount for the accredited certificate program in election administration or cybersecurity for the year.

(d) ADDITIONAL DEFINITIONS.—In this section:

(1) ACCREDITED CERTIFICATE PROGRAM IN ELECTION ADMINISTRATION OR CYBERSECURITY.—The term "accredited certificate program in election administration or cybersecurity" means a program in election administration or cybersecurity that leads to a certificate, or other nondegree recognized credential, at an eligible institution.

(2) ELIGIBLE INSTITUTION.—The term "eligible institution" means an institution of higher education (as defined under section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) that—

(A) offers an accredited certificate program in election administration or cybersecurity; and

(B) elects to participate in the program established under this section.

(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section—

(1) $1,000,000 for fiscal year 2021; and

(2) such sums as may be necessary for each of fiscal years 2022 through 2028.

From: Colleen McCormack
To: Bhanu Pothugunta; Keval Patel
Subject: Statewide Checklist Report
Date: Thursday, September 27, 2018 9:15:06 AM

Bhanu,

I thought I emailed you about the retention for the statewide checklist reports, but I cannot find the email. I apologize, I forgot to email you.

Please have a retention time of 10 days for the statewide checklist report.

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

From: Colleen McCormack
To: John Penney
Subject: Statewide Checklist
Date: Tuesday, February 19, 2019 10:57:33 AM

John,

The Statewide checklist ran on 02/12/2019. Did you save it?

It is running once a month from now on through April, until I update the election dates.

Let me know if you did save it.

Thanks

Thank You,

Colleen

Colleen E. McCormack

HAVA

Department of State

State House, Room 204 - 107 North Main St

Concord, NH 03301-4989

NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

NASS Summary: Election Security Act of 2019 (no bill number yet)

May 14, 2019

Sponsors: Rep. Bennie Thompson (D-MA), Rep. Zoe Lofgren (D-CA)

Promoting Accuracy, Integrity, and Security Through Voter Verified Permanent Paper Ballot

Voter Verified Paper Ballot Requirement

- All voting systems must use voter verified paper ballots that are marked by the voter or a ballot marking device and counted by hand, optical scanner, or other counting device. The voting system must provide the voter with the opportunity to inspect, verify, and correct any errors on the ballot before it is cast and counted.
- The voting system must not preserve the paper ballot in any way that makes it possible after the vote is cast to associate a voter with the record of the voter's vote without the voter's consent.
- The paper ballots must be preserved and counted by hand in any recount or audit. If there is a discrepancy between the electronic vote tally and the paper ballot hand count tally, the hand count tally will be the correct record of votes cast.
- If any audit, recount, or election contest shows clear and convincing evidence that a sufficient number of paper ballots have been compromised that could change the results of the election, the determination of the appropriate remedy must be made in accordance with state law, except that the electronic tally must not be used as the exclusive basis for determining the official certified result.
- All paper ballots must be printed on durable paper. Paper is durable if it can withstand multiple counts and recounts and still retain the information printed on them for a 22-month retention period.
- All paper ballots completed through a ballot marking device must be clearly readable by the voter without assistance and by an optical character recognition device or other device equipped for individuals with disabilities.
- Beginning January 1, 2021, all paper ballots must be printed on recycled paper. Paper ballots must be printed on paper manufactured in the United States.

Study and Report on Optimal Ballot Design

- The EAC must conduct a study of the best ways to design ballots, including paper ballots and electronic or digital ballots, to minimize confusion and user errors. The EAC must report to Congress on the study Accessible Voting Machines
- Individuals with disabilities must be given an equivalent opportunity to vote, including privacy and independence, in a manner that produces a voter verified paper ballot as for other voters.
- HAVA voting system requirements for individuals with disabilities may be met through the use of at least one voting system at each polling place that:
    - is equipped with nonvisual and enhanced visual accessibility for the blind and visually impaired, and nonmanual and enhanced manual accessibility for the mobility and dexterity impaired;
    - allows the voter to privately and independently verify the paper ballot through the accessible presentation of the same printed or marked vote selections that will be used for vote counting and auditing; and
    - allows the voter to verify and cast the paper ballot without requiring the voter to manually handle the paper ballot.

Study and Report on Accessible Paper Ballot Verification

- The Director of the National Science Foundation must make grants available to at least 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot verification for individuals with disabilities, voters whose primary language is not English, and voters with difficulties in literacy.
- An entity is eligible to receive a grant if it submits to the NSF an application that certifies that it will investigate enhanced methods or devices and complete the activities by December 31, 2020.
- Any technology developed with the grants must be considered non-proprietary and be made publicly available.
- $5 million is authorized to be appropriated to the National Science Foundation.

Implementation Deadlines

- The paper ballot voting system requirements apply beginning with elections held in 2022, except that states voting systems that use a paper record printer attached to a DRE or other voting system that uses or produces a verifiable paper record of the vote may delay implementation of paper ballot voting systems until the 2024 election.
- Jurisdictions which delay the implementation of paper ballot voting systems until 2024 must provide voters with the opportunity to mark and cast a paper ballot. Election officials must ensure (to the greatest extent practicable) that the waiting period for individuals to cast a paper ballot is the lesser of 30 minutes or the average wait period of a voter who does not use a paper ballot. Any paper ballot cast under these provisions must be treated as a regular ballot for all purposes. Election officials must display prominent notice that paper ballots are available. The chief state election official must ensure that polling place election officials are aware of the optional paper ballot requirements.

Voting System Security Improvement Grants

Grants for Paper Ballot Voting Systems and Election Security Improvements

- The EAC must make grants to states for replacing voting systems that do not meet the requirements of the Voter Confidence and Increased Accessibility Act and the voluntary voting system guidelines, to carry out voting system security improvements (described below), and to implement and model best practices for ballot design, ballot instructions, and the testing of ballots. The provisions must be implemented by the 2020 election.
- The EAC must determine the appropriate grant amount, except that it may not be less than the product of $1 and the average of the number of individuals who cast votes in any of the two most recent regularly scheduled general elections for Federal office in the state.
- The EAC must make pro rata reductions as necessary to ensure the entire amount appropriated is distributed to states.
- If the amount of funds appropriated exceeds the amount necessary to meet the grant requirements, the EAC must consider the following in making a determination to award remaining funds to a state:
    - The record of the state in carrying out the following:
        - providing voting machines that are less than 10 years old;
        - implementing strong chain of custody procedures for the physical security of voting equipment and paper records;

        - conducting pre-election testing on every voting machine and ensuring that paper ballots are available wherever electronic machines are used;
        - maintaining offline backups of voter registration lists;
        - providing a secure voter registration database that logs requests submitted to the database;
        - publishing and enforcing a policy detailing use limitations and security safeguards to protect the personal information of voters in the voter registration process;
        - providing a secure processes and procedures for reporting vote tallies;
        - providing a secure platform for disseminating vote totals;
        - evidence of established conditions of innovation and reform in providing voting system security and the proposed plan of the State for implementing additional conditions;
        - evidence of collaboration between relevant stakeholders;
        - the plan of the State to conduct a rigorous evaluation of the effectiveness of the activities carried out with the grant.
- To the greatest extent practicable, an eligible state which receives a grant to replace a voting system must ensure that the replacement system is capable of administering a system of ranked choice voting under which each voter shall rank the candidates for the office in the order of the voter's preference.
- Voting system security improvements for purposes of the receiving grant funds are any of the following:
    - the acquisition of goods and services from qualified election infrastructure vendors;
    - cyber and risk mitigation training;
    - a security risk and vulnerability assessment of the state's election infrastructure carried out by a provider of cybersecurity services under a contract entered into between the chief state election official and the provider;
    - the maintenance of election infrastructure, including addressing risks and vulnerabilities;
    - providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure;
    - enhancing the cybersecurity and operations of the information technology infrastructure;
    - enhancing the cybersecurity of voter registration systems;
- For the purposes of voting system security improvements, a "qualified election infrastructure vendor" is any person who provides, supports, or maintains infrastructure on behalf of a state, local government, or election agency that meet requirements established by the EAC and DHS, which must include the following criteria:
    - the vendor must be owned and controlled by a citizen or permanent resident of the US;
    - the vendor must disclose to the EAC and DHS, and the relevant chief state election official any sourcing outside the US for parts of the election infrastructure;
    - the vendor agrees to ensure that the election infrastructure will be developed and maintained in a manner consistent with cybersecurity best practices issued by the TGDC;
    - the vendor agrees to maintain its information technology infrastructure in a manner consistent with the cybersecurity best practices provided by the EAC and DHS;

- the vendor agrees to meet the requirements for reporting any known or suspected cybersecurity incidents involving any of the goods and services provided by the vendor;
- the vendor agrees to permit independent testing by the EAC and DHS of the goods and services provided.

- A vendor meets the relevant reporting requirements if, upon becoming aware of the possibility that an election cybersecurity incident has occurred involving any of the goods and services provided pursuant to the grant:
  - the vendor promptly assesses whether or not such an incident occurred and submits the required notification to the EAC and DHS of the assessment as soon as practicable, but no later than 3 days after the vendor first becomes aware of the possibility that the incident occurred;
  - if the incident involves goods or services provided to an election agency, the vendor submits a notification meeting the applicable requirements to the agency as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred), and cooperates with the agency in providing any other nec1essary notifications relating to the incident; and
  - the vendor provides all necessary updates to any notification submitted as required;
- Each required notification from a vendor must contain the following information with respect to any election cybersecurity incident covered by the notification:
  - the date, time, and time zone when the election cybersecurity incident began, if known;
  - the date, time, and time zone when the election cybersecurity incident was detected;
  - the date, time, and duration of the election cybersecurity incident;
  - the circumstances of the election cybersecurity incident, including the specific election infrastructure systems believed to have been accessed and information acquired, if any;
  - any planned and implemented technical measures to respond to and recover from the incident;
  - in the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.
- a state is eligible to receive a grant if it submits to the EAC an application describing how it will use the grant to carry out the activities and a certification not later than 5 years after receiving the grant the state will carry out risk-limiting audits.
- Not later than 90 days after the end of each fiscal year, the EAC must submit a report to the appropriate congressional committees on the activities carried out with the grant funds.
- Authorizes $1 billion for FY 2019 and $175 million for FY 2020, 2022, 2024, and 2026 for the voting system security improvement grants.

<u>DHS Membership on EAC Board of Advisors and TGDC</u>

- Expands the Board of Advisors and TGDC membership to include a representative from DHS.

<u>EAC Studies</u>

- Requires the EAC to consult with DHS on periodic studies, as appropriate.
- Requires that the goal of EAC studies include promoting election methods that are secure against attempts to undermine the integrity of election systems by cyber or other means.

<u>Use of Requirements Payments</u>

- Allows states to use a requirements payment to carry out any of the following activities:
    - cyber and risk mitigation training;
    - providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure;
    - enhancing the cybersecurity and operations of the information technology infrastructure;
    - enhancing the security of voter registration databases

State Plan Description Update

- Requires that the state plan description of how the state will use requirements payments to improve the administration of elections include the protection of election infrastructure.

Composition of State Plan Committee

- Updates the composition of the committee responsible for developing the state plan to require the membership be a representative group of individuals from the state's counties, cities, towns, and Indian tribes, and represent the needs of rural as well as urban areas of the state.

Protection of Voter Registration List

- Requires that the technology measures for securing the voter registration list include measures to prevent and deter cybersecurity incidents, as identified by the EAC, DHS, and the TGDC.

Grants for Risk-Limiting Audits of Results of Elections

Grants for Risk-Limiting Audits

- Requires that the make grants to states to conduct risk limiting audits with respect to the 2020 election and each succeeding election
- A risk-limiting audit is a post-election process:
    - conducted in accordance with rules and procedures established by the chief state election official of the state which meet the applicable requirements;
    - under which, if the reported outcome of the election is incorrect, there is at least a predetermined percentage chance that the audit will replace the incorrect outcome with the correct outcome as determined by a full, hand-to-eye tabulation of all votes validly cast in that election that ascertains voter intent manually and directly from voter verifiable paper records.

Risk-Limiting Audit Requirements

- Rules and procedures established for conducting a risk-limiting audit must include the following elements:
    - rules for ensuring the security of ballots and documenting that prescribed procedures were followed;
    - rules and procedures for ensuring the accuracy of ballot manifests produced by election agencies;
    - rules and procedures for governing the format of ballot manifests, cast vote records, and other data involved in the audit;
    - methods to ensure that any cast vote records used in the audit are those used by the voting system to tally the election results sent to the chief state election official and made public;
    - procedures for the random selection of ballots to be inspected manually during each audit;

- rules for the calculations and other methods to be used in the audit and to determine whether and when the audit of an election is complete;
- procedures and requirements for testing any software used to conduct risk-limiting audits.

- The term "ballot manifest" means a record maintained by each election agency that meets each of the following requirements:
  - the record is created without reliance on any part of the voting system used to tabulate votes;
  - the record functions as a sampling frame for conducting a risk-limiting audit;
  - the record contains the following information with respect to the ballots cast and counted in the election:
    - the total number of ballots cast and counted by the agency (including undervotes, overvotes, and other invalid votes)
    - the total number of ballots cast in each election administered by the agency (including undervotes, overvotes, and other invalid votes)
    - A precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.
- The term "incorrect outcome" means an outcome that differs from the outcome that would be determined by a full tabulation of all votes validly cast in the election, determining voter intent manually, directly from voter-verifiable paper records.
- The term "outcome" means the winner of an election, whether a candidate or a position.
- The term "reported outcome" means the outcome of an election which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.

<u>Eligibility for Risk-Limiting Audit Grant</u>

- A state is eligible to receive a grant by submitting an application to the EAC that includes:
  - A certification that, no later than 5 years after receiving the grant, the state will conduct risk limiting audits of the results of elections for federal office;
  - a certification that, no later than one year after the date of enactment, the chief state election official of the state has established or will establish the rules and procedures for conducting the audits which meet the requirements;
  - a certification that the audit will be completed no later than the date on which the state certifies the results of the election;
  - a certification that, after completing the audit, the state will publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly;
  - a certification that, if a risk-limiting audit leads to a full manual tally of an election, state law requires that the state or election agency use the results of the full manual tally as the official results of the election

<u>Authorization of Appropriations</u>

- Authorizes to be appropriated for risk limiting audit grants $20 million for fiscal year 2019.

GAO Analysis

- No later than 6 months after the first election for federal office held after grants are first awarded to states for conducting risk-limiting GAO must conduct an analysis of the extent to which the audits have improved the administration of such and the security of election infrastructure.

Security Measures

Election Infrastructure Definition

- Amends the Homeland Security Act to define "election infrastructure" as storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office, as well as related information and communications technology, including voter registration databases, voting machines, electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results), and other systems used to manage the election process and to report and display election results on behalf of an election agency.

Election Infrastructure Designation

- Amends the Homeland Security Act to include election infrastructure as part of the government facilities critical infrastructure sector.

DHS Responsibilities

- Updates the DHS Secretary's responsibilities relating to intelligence and analysis to include providing timely threat information regarding election infrastructure to the chief state election official of the pertinent state.

Security clearance assistance for election officials

- Provides that in order to promote the timely sharing of information on threats to election infrastructure, DHS may:
    - help expedite a security clearance for the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official;
    - sponsor a security clearance for the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official; and
    - facilitate the issuance of a temporary clearance to the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official, if DHS determines classified information to be timely and relevant to the election infrastructure of the state at issue

Security risk and vulnerability assessments

- No later than 90 days after receiving a written request from a chief state election official, the DHS must, to the extent practicable, commence a security risk and vulnerability assessment on election infrastructure in the state at issue.
- If DHS determines that a security risk and vulnerability assessment cannot be commenced within 90 days, it must expeditiously notify the chief state election official who submitted the request.

Report on DHS Assistance

- No later than one year after the date of the enactment and annually thereafter through 2026, DHS must submit to Congress a report on:
    - efforts to carry out the security clearance assistance provisions during the prior year, including specific information on which states were helped, how many officials have been helped in each state, how many security clearances have been sponsored in each state, and how many temporary clearances have been issued in each state; and
    - efforts to carry out the risk and vulnerability assessment provisions during the prior year, including specific information on which states were helped, the dates on which the DHS received a request for a security risk and vulnerability assessment, the dates on which DHS commenced request, and the dates on which DHS transmitted a notification as required.

Report on Foreign Threats

- No later than 90 days after the end of each fiscal year (beginning with fiscal year 2019), DHS and the Director of National Intelligence, in coordination with the heads of appropriate offices of the Federal government, must submit a report to the appropriate congressional committees on foreign threats to elections in the US, including physical and cybersecurity threats.

Report on Assistance from States

- For the purpose of preparing the above reports DHS must solicit and consider information and comments from states and election agencies, except that providing the information and comments by a state or election agency must be voluntary and at the discretion of the state or agency.

Pre-Election Threat Assessments

- No later than 180 days before the date of each election Director of National Intelligence must submit an assessment of the full scope of threats to election infrastructure, including cybersecurity threats posed by state actors and terrorist groups, and recommendations to address or mitigate the threats, as developed by DHS and the EAC to each chief state election official and relevant Congressional committee.
- If, at any time after submitting an assessment the Director of National Intelligence determines that the assessment should be updated to reflect new information regarding the threats involved, the Director must submit a revised assessment.

Enhancing Protections for United States Democratic Institutions

National Strategy to Protect US Democratic Institutions

- No later than one year after the date of enactment the President must issue a national strategy to protect against cyber-attacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of US democratic institutions. The national strategy must include consideration of the following:
    - the threat of a foreign state actor, foreign terrorist organization or a domestic actor carrying out a cyber-attack, influence operation, disinformation campaign, or other activity;
    - the extent to which US democratic institutions are vulnerable to a cyber-attack, influence operation, disinformation campaign, or other activity;
    - potential consequences that could result from a successful cyber-attack, influence operation, disinformation campaign, or other activity;
    - lessons learned from other Western government institutions which were subject to a cyber-attack, influence operation, disinformation campaign, or other activity;

- potential impacts an erosion of public trust in democratic institutions as could be associated with a successful cyber breach or other activity negatively affecting election infrastructure;
- roles and responsibilities of DHS, EAC, other federal and non-federal entities, including election officials, and representatives of a multi-state information sharing and analysis center;
- any findings, conclusions, and recommendations to strengthen protections for US democratic institutions that have been agreed to by a majority of members on the National Commission to Protect United States Democratic Institutions

- No later than 90 days after issuance of the national strategy, the President must issue an implementation plan for federal efforts to implement the strategy that includes:
  - strategic objectives and corresponding tasks
  - projected timelines and costs for the tasks
  - metrics to evaluate performance of the tasks

National Commission to Protect United States Democratic Institutions

- Establishes within the legislative branch the National Commission to Protect United States Democratic Institutions to counter efforts to undermine democratic institutions within the US.
- The Commission must be composed of 10 members appointed for the life of the Commission as follows:
  - one member appointed by DHS;
  - one member appointed by the EAC;
  - two members appointed by the majority leader of the Senate;
  - two members appointed by the minority leader of the Senate;
  - two members appointed by the Speaker of the House of Representatives;
  - two members appointed by the minority leader of the House of Representatives
- Individuals must be selected for appointment to the Commission solely on the basis of their professional qualifications, achievements, public stature, experience, and expertise in relevant fields, including, but not limited to cybersecurity, national security, and the U.S. Constitution.
- No later than 18 months after the date of the first meeting the Commission must submit to the President and Congress a final report containing the findings, conclusions, and recommendations to strengthen protections for democratic institutions in the US as have been agreed to by a majority of the members of the Commission.
- The Commission must terminate within 60 days of submitting the final report.

Promoting Cybersecurity Through Improvements in Election Administration

Compliance Testing of Existing Voting Systems

- Requires that no later than 9 months before a federal election the EAC provide for testing by an accredited laboratory of the voting system hardware and software certified for use in the most recent election, based on the most recent applicable voting system guidelines.
- If any voting system hardware of software does not meet the most recent guidelines based on the testing, it must be decertified by the EAC.
- The above requirements apply beginning with the 2020 election.

TGDC Cybersecurity Guidelines

- Requires that no later than 6 months after enactment the TGCD issue election cybersecurity guidelines including standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.

Electronic Boll Book Treatment

- Amends HAVA to treat electronic poll books as part of a voting system and defines electronic poll books as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) used to retain the list of registered voters at a polling location, or vote center, or other location at which voters cast votes in an election and to identify registered voters who are eligible to vote in an election.
- The above provision applies with respect to any requirements relating to electronic poll books on and after January 1, 2020.

Pre-Election Reports on Voting System Usage

- Requires that no later than 120 days before the date of each federal election the chief state election official submit a report to the EAC containing a detailed voting system usage plan for each jurisdiction in the state which will administer the election, including a detailed plan for the usage of electronic poll books and other equipment and components of such system.
- The above provision applies beginning with the 2020 election.

Preventing Election Hacking

Bug Bounty Program

- No later than 1 year after enactment of this Act, DHS must establish a program to be known as the ''Election Security Bug Bounty Program'' to improve the cybersecurity of the systems used to administer elections by facilitating and encouraging assessments by independent technical experts, in cooperation with state and local election officials and election service providers, to identify and report election cybersecurity vulnerabilities.
- Participation in the program by state and local election officials and election service providers is voluntary.
- In developing the program DHS must solicit input from, and encourage participation by, state and local election officials.
- In establishing and carrying out the program, DHS must:
    - establish a process for state and local election officials and election service providers to voluntarily participate;
    - designate appropriate information systems to be included;
    - provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems and establish criteria to be considered eligible such compensation;
    - consult with DOJ on how to ensure that approved individuals, organizations, or companies are protected from prosecution and liability for specific activities authorized under the program;
    - consult with DOD and other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from the programs;

- develop an expeditious process by which an individual, organization, or company can register with DHS, submit to a background check, and receive a determination as to eligibility for participation in the program;
- engage qualified interested persons, including representatives of private entities, about the structure of the program and, to the extent practicable, establish a recurring competition for independent technical experts to assess election systems for the purpose of identifying and reporting election cybersecurity vulnerabilities

- DHS may award competitive contracts as necessary to manage the program.

Election Security Grants Advisory Committee

- Establishes an advisory committee to assist the EAC with the award of grants to states under the Act for the purpose of election security. The Committee must review grant applications received by the EAC and recommend to the EAC whether to award the grant to the applicant. In reviewing an application, the Committee must consider:
  - the record of the applicant with respect to compliance of the applicant with the requirements under subtitle A of title III and adoption of voluntary guidelines issued by the EAC under subtitle B of title III; and the goals and requirements of election security as described in title III.
  - the Committee must be composed of 15 individuals appointed by the Executive Director of the EAC with experience and expertise in election security.
- The advisory committee requirement takes effect 1 year after the date of enactment.

Use of Voting Machines Manufactured in the United States

- No later than the November 202 election each state must seek to ensure that any voting machine used in the election and in any subsequent election is manufactured in the United States.

Report on Adequacy of Resources for Implementation

No later than 120 days after enactment of the Act, the EAC and DHS must submit a report to the relevant Congressional committees analyzing the adequacy of the funding, resources, and personnel available to carry out the Act.

NASS Summary of HR 1 For the People Act
(Provisions concerning election administration)
As of March 13, 2019

Contents:

Election Access

A. Voter Registration Modernization

1. Promoting Internet Registration

Availability of Online Voter Registration

- States must ensure that the appropriate election officials provide the public with the ability to submit a voter registration application online, and have it accepted online. The system must provide applicants with online assistance with registering to vote, and must provide for online completion and submission of the National Mail Voter Registration Form, including assistance with providing an electronic signature.
- States must accept an online voter registration application and ensure an individual is registered to vote if the individual meets the same registration requirements applicable to individuals who register to vote by mail using the National Mail Voter Registration Form and, for applications submitted during or after the second year that the bill has been in effect, the individual provides an electronic signature.
- States must ensure that an individual is registered to vote if the person submits a valid online voter registration application no later than the lesser of 30 days, or the period provided by state law, prior to the election.

Availability of Telephone System

- In addition to online registration, states must provide an automated telephone-based system that provides the same services as the online registration system.

Accessibility of Services

- A state shall ensure that the services made available under this section are made available to individuals with disabilities to the same extent as services are made available to all other individuals.

Signature Requirements

- An individual meets the signature requirements if:
    - the individual consents to the transfer of an electronic signature on file with a state agency required to provide voter registration services, including the state motor vehicle authority;
    - If the above does not apply, the individual submits an electronic copy of the handwritten signature through electronic means with the application;
    - If neither of the above apply, the individual makes a computerized mark in the signature field of the online application, in accordance with reasonable security measures established by the state, and only if the state accepts the mark.
- If an individual is unable to meet any of the above signature requirements, the state must ensure the individual is registered to vote if the individual completes all other elements of the online application and provides a signature at the time the individual requests a ballot (whether by mail or at a polling place).
- The state must ensure that individual applying to register online are notified of the signature requirements and the options for those unable to meet those requirements.

Security Measures

- The state must establish appropriate security measures to prevent, to the greatest extent practicable, unauthorized access to the registration information submitted online.

Notices

- The state must provide an individual with notice confirming receipt of a completed online application and instructions on checking the status of the application. The state must send the individual a notice of disposition no later than 7 days after the application has been accepted or rejected. The notices must be sent by mail, and by email if requested by the individual.

HAVA Identification Requirement

- Individuals who register to vote online and have not voted in a federal election must comply with the applicable identification requirements under HAVA and, with certain exceptions (see p. 24), must provide a handwritten signature.

Updating Online Voter Registration Information

- The appropriate state or local election official must ensure that any registered voter may update the voter's registration information online, including the voter's address and email address. A voter must attest to the update by providing an electronic signature. The election official must send the individual a notice confirming receipt of the application with instructions on checking the status of the update. The election official must also send a notice of disposition no later than 7 days after the update has been accepted or rejected. The notices must be sent by mail, and by email if requested by the individual.
- If updated registration information affects a voter's eligibility to vote in an upcoming federal election, the appropriate election official must ensure that the information is processed with respect to that election if the voter updates the information no later than the lesser of 7 days, or the period provided by state law, prior to the election.
- A notice sent by election officials under NVRA to confirm a registered voter's change of address must indicate that the voter may update their registration information online as a way to confirm that voter did not move or moved within the jurisdiction.

Collection of Email Addresses

- Requires that the National Mail Voter Registration Form include a space for an email address (at the applicant's option), along with a statement that if the applicant's so requests, election officials will send the same voter registration and voting information that would be sent by mail to that email address. The state election official must ensure that any email addresses provided are used only for the purpose of official election duties.
- If an email address is provided on the mail registration form for the purpose of receiving voting information, election officials must send the voter an email no later than 7 days before an election notifying the voter how they can obtain, through electronic means, the name, address, and hours of the voter's polling place, and information on identification requirements.

Clarification on Information to Show Eligibility

- For the purpose of meeting NVRA deadlines for submitting a voter registration application, a state must consider an application as valid if the applicant substantially completes the application attests to the required statement, and, if the application is submitted online, provides a signature in accordance with applicable requirements.

Effective Date

- The voter registration modernization provisions would take effect on January 1, 2020. Subject to the approval of the EAC, if a state certifies to the EAC that it will not meet the effective date because of extraordinary circumstances, and includes the reasons for failing to meet the deadline, the state will have until January 1 2022 to comply with the provisions.

2. Automatic Voter Registration

Automatic Voter Registration Requirements

- Each chief state election official must implement an automatic registration system. The term "automatic registration" means a system that registers eligible individuals to vote in federal elections by electronically transferring voter registration information from government agencies to the state election official so that an individual will be registered to vote, unless the individual affirmatively declines.

Contributing Agencies

- Each chief state election official must publish on the public website of the official an updated listing of all contributing agencies in the state no later than 180 days before each election.
- The following agencies in each state must be treated as a contributing agency:
    - each agency that is required by federal law to provide voter registration services, including the state motor vehicle authority and other voter registration agencies NVRA;
    - each agency that administers a program under applicable sections of the Social Security Act or the Patient Protection and Affordable Care Act;
    - each agency primarily responsible for regulating the private possession of firearms;
    - each state agency primarily responsible for maintaining identifying information for students enrolled at public secondary schools, including, where applicable, the agency responsible for maintaining the education data system described in the America COMPETES Act
    - in the case of a state in which an individual disenfranchised by a criminal conviction may become eligible to vote upon completion of a criminal sentence or any part thereof, or upon formal restoration of rights, the state agency responsible for administering that sentence, or part thereof, or restoration of rights;
    - other agency designated by the state as a contributing agency
- The following federal agencies must be treated as a contributing agency with respect to individuals who are residents of that state:
    - the Social Security Administration, the Department of Veterans Affairs, the Defense Manpower Data Center of the Department of Defense, the Employee and Training Administration of the Department of Labor, and the Center for Medicare & Medicaid Services of the Department of Health and Human Services;
    - the Bureau of Citizenship and Immigration Services, but only with respect to individuals who have completed the naturalization process;
    - in the case of an individual who is a resident of a state in which an individual disenfranchised by a criminal conviction under federal law may become eligible to vote upon completion of a criminal sentence or any part thereof, or upon formal restoration of rights, the federal agency responsible for administering that sentence or part thereof (without regard to whether the agency is located in the same state in which the individual is a resident), but only with respect to individuals who have completed the criminal sentence or any part thereof;

- any other agency of the federal government which the state designates as a contributing agency, but only if the state and the head of the agency determine that the agency collects information sufficient to carry out the responsibilities of a contributing agency.

- Special Rule for Institutions of Higher Education

  Each institution of higher education must be treated as a contributing agency except that the institution must be treated as a contributing agency only if, in its normal course of operations, it requests each student registering for enrollment in a course of study, including enrollment in a program of distance education, to affirm whether or not the student is a US citizen, and if the institution is treated as a contributing agency in a state, the institution shall serve as a contributing agency only with respect to students, including students enrolled in a program of distance education, who reside in the State. For these purposes an institution of higher education is one which has a program participation agreement in effect with the Secretary of Education and which is located in a state to which section 4(b) of NVRA does not apply.

Contributing Agencies Collaboration with State

- Each state and federal agency and institution of higher education required to be treated as a contributing agency in a state must assist the chief state election officials in registering to vote all eligible individuals served by that agency.
- Each chief state election official must in collaboration with each contributing agency take appropriate measures to educate the public about the automatic voter registration procedures.

Contributing Agency Assistance

- Each contributing agency that requests that individuals affirm US citizenship with each application for service or assistance (or other specified transaction) must inform each individual of the following:
  - that the individual will be registered to vote (or registration updated) unless the individual declines or is found ineligible;
  - the substantive qualifications for an elector based on the national mail registration form, the consequences of false registration, and that the individual should decline to register if the individual does not meet all the qualifications;
  - where applicable, the requirement that the individual must affiliate or enroll with a political party in order to participate in the election;
  - that voter registration is voluntary and neither registering or declining to register will affect the availability of services or benefits.
- Each contributing agency must ensure that no application for service or assistance (or other specified transaction) can be completed until the individual is given the opportunity to decline to be registered to vote.

Transmittal of Information from Contributing Agency

- Upon expiration of the 30-day period beginning on the date the contributing agency informs the individual, each contributing agency must transmit to the state, unless the individual declines registration during that period, in a format compatible with the state voter registration database:
  - the individuals name, date of birth, and residential address;
  - information confirming US citizenship;
  - the date the individual's information was collected;
  - the individual's signature in electronic form (if available)

- information regarding the individual's affiliation or enrollment with a political party (if provided)
- and additional information listed in the national mail voter registration form

- Each contributing agency that in the normal course of operations does not request individuals apply for service or assistance (or other specified transaction) to confirm US citizenship must complete the relevant NVRA requirements regarding the mail registration form and ensure each applicant's transaction cannot be completed until the applicant indicates whether the applicants wishes to register or declines to register. If the individual registers the information must be transmitted in accordance with the above provisions.
- Each contributing agency must offer each individual with each application for service or assistance (or other specified transaction) the opportunity to register as provided above regardless of whether the individual previously declined a registration opportunity.
- No later than 15 days after a contributing agency has transmitted the relevant information, the state election official must ensure the individual is registered to vote and not later than 120 days after a contributing agency has transmitted such information with respect to the individual, send written notice to the individual of the individual's registration status.

Registration Based on Existing Contributing Agency Records

- Each contributing agency must transmit to the state election official no later than the effective date the relevant information for each individual listed in the agency's existing records as of the date of enactment. The agency must transmit information for individuals listed in the records as of the effective date but not the date of enactment no later than 6 months after the effective date.
- After a contributing agency transfers the information on individuals in its existing records to the state, each state election official must identify all individuals who are eligible to be, but are not currently registered to vote and send each of the individuals a written notice that informs the individual of the following:
  - that voter registration is voluntary but if the individual does not decline registration the individual will be registered;
  - a statement offering the opportunity to decline registration;
  - the substantive qualifications for an elector based on the national mail registration form, and a statement that the individual should decline to register if the individual does not meet all the qualifications;
  - where applicable, the requirement that the individual must affiliate or enroll with a political party in order to participate in the election;
  - instructions for correcting any erroneous information;
  - instructions for providing any additional information listed in the national mail registration form.
- Each state election official must ensure that each such eligible individual is registered to vote no later than 45 days after sending the official sending the above notice, unless during the 30-day period beginning on the date the notice is sent the individual declines registration in writing, through internet communication, or officially logged telephone communication. Each state election official must also send written notice to each such individual of the individual's voter registration status.
- States may not refuse to treat an individual as eligible because the individual is less than 18 at the time a contributing agency receives information with respect to the individual as long as the individual is at least 16 years of age.

Voter Protection and Security

- An individual must not be prosecuted under federal or state law or adversely affected in legal proceedings concerning immigration status or citizenship based on certain errors in automatic registration process or because the individual declined voter registration or did not make an affirmation of citizenship. Declining voter registration or not affirming citizenship may not be used as evidence against an individual in any law enforcement proceeding. Legal actions based on certain actions or statements made knowingly and willfully are not restricted.
- Contributing agencies are not authorized to collect, retain, transmit, or publicly disclose an individual's decision to decline voter registration, a decision not to affirm citizenship, or any of the information transmitted to the state, except in the ordinary course of business.
- States are restricted from publicly disclosing certain information received from a contributing including any portion of the individual's SSN or driver's license number, signature, telephone number, and email.
- States must maintain and make publicly available, including in electronic form and through electronic methods, all records of changes to voter records, including removals, the reasons for removals, and updates, for 2 years.

NIST Database Management Standards

- NIST must establish and publish standards governing comparison of data for voter registration and list maintenance purposes that address specific criteria, including specific data elements, matching rules, use of data to determine ineligibility and determining a record to be a duplicate or outdated. The standards must be published not later than 45 days after the deadline for public notice and comment.

NIST Privacy and Security Standards

- NIST must develop and publish privacy and security standards that require the chief state election official to adopt a policy that specifies each class of users with access to the statewide voter registration list and associated permissions and levels of access, sets forth safeguards to protect the privacy, security and accuracy of the list, and specifies safeguards to protect personal information transmitted through the automatic registration procedures. The standards must be published not later than 45 days after the deadline for public notice and comment.
- The CEO of each state must annually file a certification with NIST that the state is in compliance with the privacy and security standards for voter registration. No state may receive payments pertaining to this part of the bill if the certification is not timely filed. If a state requires changes in state law to implement the NIST standards the state may make the certification for no more than 2 years and must submit an addition certification once legislation is enacted.
- Each state election official must publish the privacy and security standards online and make available in written form.
- Prohibits discrimination against an individual based on voter registration records, declination to register or affirm citizenship under automatic registration procedures, or voter registration status, and prohibits unauthorized use of that information.
- Prohibits use of voter registration information collected under the above provisions may be used for commercial purposes. Does not prohibit transmission, exchange, or dissemination for political purposes.

Registration Portability and Correction

- If an individual is registered for an election the election officials at the polling place must permit the individual to update the individual's address, correct any incorrect information, and cast a ballot based on the update or correct information that is treated as a regular ballot and not provisional.

- Polling place officials must ensure that any updated or corrected information is promptly entered into the state voter registration system.

Payments and Grants

- Authorizes a total of $500 million for FY 2019 and such sums as necessary for succeeding years for the EAC to make grants to states to assist in implementing the automatic voter registration provisions, or, for exempt states, implementing the existing automatic voter registration program.
- An exempt state is one that already operates an automatic voter registration program. Exempt states must still comply with certain provisions.
- To receive a grant states must submit to the EAC an application containing a description of the activities that will be carried out with the grant, assurances that the activities will be carried out without partisan bias, and any other information required by the EAC.
- The EAC must determine the grant amounts made to an eligible state, giving priority to funds for activities most likely to accelerate compliance with the requirements, including investments supporting electronic information transfer between contributing agencies and the state, updates to online voter registration systems, introduction of online voter registration systems, and public education on new methods of voter registration, and updating or correcting voter registration.

Miscellaneous Provisions

- Contributing agencies must ensure services are provided to individuals with disabilities to the same extent as other individuals. Services must be made in a nonpartisan and nondiscriminatory manner and comply with applicable laws.
- Contributing agencies are not prohibited from contracting with a third party to assist the agency in meeting information transmittal requirements, provided applicable requirements are met.
- States may send required notices via email if the individual has provided an email and consented to email communications for election materials.
- NVRA provision regarding civil enforcement and private right of action apply to these provisions.

Effective Date

- The automatic voter registration requirements apply with respect to a state beginning January 1, 2021.
- States may seek a waiver from the EAC if it certifies to the EAC that it will not meet the deadline because of extraordinary circumstances and includes the reasons for failing to meet the deadline.

3. Same Day Voter Registration

Same Day Registration Availability

- On the day of a federal election, and on any day when voting, including early voting, is permitted for a federal election, each state must permit any eligible voter to register to vote in the election at the polling place using a form that meets the requirements of NVRA, or revise information if already registered, and cast a vote in the election. This requirement does not apply to a state in which there is no voter registration requirement with respect to elections for federal office.

Effective Date

- Each state must comply with this requirement beginning with the general election for federal office in November 2020.

4. Conditions on Removal on Basis of Interstate Cross Check

Conditions on Removal of Registrants from List of Eligible Voters on Basis of Interstate Cross-Checks

- To the extent that the program carried out by a state under NVRA to systematically remove the names of ineligible voters from the official lists of eligible voters uses information obtained in an interstate crosscheck, in addition to any other conditions imposed under the Act on the authority of the state to remove the name of the voter from such a list, the state may not remove the name of the voter from the list unless:
    - the state obtained the voter's full name (including the voter's middle name, if any) and date of birth, and the last 4 digits of the voter's SSN, in the interstate cross-check; or
    - the state obtained documentation from the ERIC system that the voter is no longer a resident of the state
- NVRA is amended to require completion of cross-checks no later than 6 months prior to the election.

Effective Date

- The above provisions apply with respect to elections held on or after the expiration of the 6-month period beginning on the date of enactment.

5. Other Initiatives to Promote Voter Registration

Annual Report on Voter Registration Statistics

- No later than 90 days after the end of each year, each state must submit to the EAC and Congress a report containing the following categories of information for the year:
    - the number of individuals who were registered under the automatic registration requirements of the Act;
    - the number of voter registration application forms completed by individuals that were transmitted by motor vehicle authorities and voter registration agencies to the chief state election official of the, broken down by each such authority and agency;
    - the number of individuals whose voter registration application forms were accepted and who were registered to vote and the number whose forms were rejected and who were not registered to vote, broken down by each such authority and agency;
    - the number of changes of address forms and other forms indicating that an individual's identifying information has been changed that were transmitted by motor vehicle authorities and voter registration agencies to the chief state election official, broken down by each such authority and agency and the type of form transmitted;
    - the number of individuals on the state voter registration list whose voter registration information was revised by the chief state election official as a result of the forms transmitted by motor vehicle authorities and voter registration agencies broken down by each such authority and agency and the type of form transmitted;
    - the number of individuals who requested the chief state election official to revise voter registration information on the list, and the number of individuals whose information was revised as a result of the request.
- In preparing the above report, the state must, for each category of information, include a breakdown by race, ~~and~~ ethnicity, age, and gender of the individuals whose information is included in the category, to the extent that information is available to the state.

Ensuring Pre-Election Registration Deadline Consistency with Legal Public Holidays

- Changes the deadlines for submitting a voter registration application under Section 8(a)(1) of NVRA from 30 days to 28 days.
- The above change goes into effect beginning with the 2020 election.

USPS Change of Address Forms to Remind Voters to Update Registration

- Requires that no later than 1 year after enactment USPS modifies hard copy change of address forms to contain a reminder to update voter registration. Requirement does not apply to electronic versions of the form.

Grants to Encourage Involvement of Minors in Election Activities

- Requires the EAC to make grants to states to carry out a plan to increase the involvement of individuals under 18 in public election activities.
- States requesting a grant must submit a plan that includes methods to promote the use of the NVRA pre-registration process (as amended by the Act); civic engagement modifications to secondary school curriculums; and other activities to encourage involvement of young people in the electoral process.
- Authorizes $25 million in grants for the program. The funds must be used over a 2-year period, after which states must submit a report to the EAC on efforts carried out using the funds.

6. Availability of HAVA Requirements Payments

Use of Requirements Payments for Implementation

- Beginning FY 2018 and each succeeding year, a state may use a requirements payment to carry out any of the requirements of the Voter Registration Modernization Act of 2019 (1-5 above) including the requirements of NVRA which are imposed by the Voter Registration Modernization Act of 2019.

7. Prohibiting Interference with Voter Registration

Prohibiting Hindering, Interfering With, or Preventing Voter Registration

- No person may corruptly hinder, interfere with, or prevent another person from registering to vote or to corruptly hinder, interfere with, or prevent another person from aiding another person in registering to vote. Any person who attempts to commit these offenses will be subject to the same penalties.
- Any person who violates this provision will be fined, imprisoned not more than 5 years, or both.

Effective Date

- The above provision applies with respect to election on or after the date of enactment.

EAC Best Practices

- No later than 180 days after date of the enactment, the EAC must develop and publish recommendations for best practices for states to use to deter and prevent violations relating to the above provisions, and section 12 of NVREA (concerning unlawful interference with registering to vote and voting) including practices to provide for the posting of relevant information at polling places and

voter registration agencies for the training of poll workers and election officials, and relevant educational materials.

HAVA Voting Information Requirement

- Voting information posted by election officials on Election Day under HAVA must include information relating to the prohibitions above and in NVRA against interfering with voting and voter registration, including information on how individuals may report allegations of violations.

8. Voter Registration Efficiency Act

Requirement for Driver's License Applicants in New State

- Requires driver's license applicants to indicate if the individual resides or resided in another state prior to applying for the license, and if so, identify the state involved and indicate whether the individual intends for the state to serve as the individual's voting residence. If the individual indicated the intent for the state to serve as the individua's residence for voting purposes, the motor vehicle authority must notify the state election official.
- The above requirements are effective beginning with election occurring in 2019.

9. Voter Registration Information to Secondary School Students

Pilot Program for Providing Voter Registration Information to Students

- Requires the EAC to carry out a pilot program to provide funds during the one-year period after the date of the enactment to eligible local educational agencies for initiatives to provide information on registering to vote in elections for public office to secondary school students in the 12th grade.
- A local educational agency is eligible to receive funds if the agency submits an application to the EAC that includes a description of the initiatives the agency intends to carry out with the funds; an estimate of the costs associated with the initiatives; and other information and assurances the EAC may require.
- A local educational agency receiving funds under the program must consult with state and local election officials in developing the initiatives the agency will carry out with the funds.
- Local education agencies must submit a report to the EAC on the initiatives carried out with the funds and the EAC must submit a report to Congress on the pilot program.
- Authorizes such sums as may be necessary for the pilot program.

10. Voter Registration of Minors

Acceptance of Voter Registration Applications from Individuals Under 18

- Prohibits states from refusing to accept a voter registration application on the grounds the individual is under 18 years of age at the time the application is submitted so long as the individual is at least 16 at that time. Does not require states to permit an individual 18 to vote in the election.
- The above requirement is effective with respect to elections occurring on or after January 1 2020.

B. Access to Voting for Individuals with Disabilities

Absentee Voting Availability for Individuals with Disabilities

- Each state must permit individuals with disabilities to use absentee registration procedures and vote by absentee ballot in federal elections, and must accept and process any otherwise valid voter registration application and absentee ballot application received by the appropriate state election official no less than 30 days before the election.

Procedures for Absentee Ballot Requests by Mail or Electronically

- States must establish procedures that allow individuals with disabilities to request voter registration applications and absentee ballot applications by mail or electronically for federal elections. The procedures must include a means for the voter to designate whether the voter wants to receive the application by mail or electronically. The state must transmit the voter registration application or absentee ballot application based on the preference selected by the voter. If the voter does not indicate a preference, the application must be delivered in accordance with state law. In the absence of any relevant state law, the application must be delivered by mail.

Procedures for Blank Ballot Delivery by Mail or Electronically

- States must establish procedures for security transmitting blank absentee ballots by mail and electronically to individuals with disabilities. The procedures must include a means for the voter to designate whether the voter wants to receive the blank ballot by mail or electronically. The state must transmit the ballot based on the preference selected by the voter. If the voter does not indicate a preference, the ballot must be delivered in accordance with state law. In the absence of any relevant state law, the ballot must be delivered by mail.

Tracking Measures for Absentee Ballots

- States must apply such methods as the state considers appropriate, such as assigning a unique identifier to the ballot, to ensure that if an individual with a disability requests the state to transmit a blank absentee ballot to the individual, the voted absentee ballot which is returned is the same blank absentee ballot which the state transmitted to the individual.

Absentee Ballot Transmission Time

- Absentee ballots must be sent at least 45 days before the election to any individual with a disability who has submitted a request by that date. If the request is received less than 45 days before the election, the ballot may be sent in accordance with state law and, if practicable, in an expedited manner.
- If a state declares or otherwise holds a runoff election, the state must establish a written plan that provides absentee ballots to individuals with disabilities in a manner that gives them sufficient time to vote.

Designation of Single Office for Absentee Voting Information

- Each state must designate a single office that is responsible for providing information regarding voter registration procedures and absentee ballot procedures to be used by individuals with disabilities with respect to federal elections.

Designation of Electronic Communication Methods

- Each state must designate at least one means of electronic communication for the following purposes: for use by individuals with disabilities to request voter registration applications and absentee ballot applications; for use by the states to send voter registration and absentee ballot applications to

individuals with disabilities; and for providing individuals with disabilities with election and voting information.

- In addition to the means of electronic communication designated by the state, the state may provide multiple means of electronic communication to individuals with disabilities, including a means of electronic communication for jurisdictions within the state.
- The state must include the designated means of electronic communication on all information and instructional materials that accompany balloting materials sent by the state to individuals with disabilities voters.

Transmission Time Waiver for Undue Hardship

- A state may request a waiver from the 45-day transit time provision if the chief state election official determines that the state cannot meet the requirements due to undue hardship. The undue hardship must be one of the following: the date of the state primary; a delay in generating ballots due to a legal contest; or provision in the state constitution that prohibit the state from complying with the time frame requirements. The waiver request must include: a recognition that the purpose of the 45 day transit time is to allow individuals with disabilities enough time to vote in federal elections; an explanation of why the state cannot meet the requirement; the number of days prior to federal elections that the state requires absentee ballots be sent to such individuals; and a comprehensive plan to ensure that such individuals are able to receive and submit an absentee ballot in time for it to be counted.
- A written waiver request must be submitted to the Attorney General no later than 90 days before the election. The Attorney General must grant the waiver request if the comprehensive plan is deemed sufficient and the Attorney General determines that an undue hardship exists. The Attorney General must approve or deny a waiver request no later than 65 days before the Election.
- If a state requests a waiver based on a delay in generating ballots due to a legal contest, the request must be submitted as soon as practicable. The Attorney General must approve or deny the request no later than 5 days after the waiver request is received.
- If a waiver request is granted, it is valid only for the election for which the request was submitted.

Effective Date

- The above provisions regarding absentee voting by individuals with disabilities apply with respect to elections held on or after January 1, 2020.

Expansion and Reauthorization of HHS Grant Program

- Reauthorizes the HHS grant program under HAVA for assuring access to individuals with disabilities is reauthorized for FY 2020, and each succeeding year, with such sums as may be necessary to carry out the program.
- The HHS grants may be used for making absentee voting and voting at home accessible to individuals with disabilities; make polling places more accessible to individuals with disabilities; and providing solutions to problems of access to voting and elections for individuals with disabilities.
- Any amounts appropriated for the HHS grant program for FY 2020 or succeeding years which have not been obligated or expended by the state or local government prior to the 4-year expiration period must be transferred to the EAC. The EAC must reallocate the funds to state or local governments that expended all funds previously received.

Pilot Program for Individuals with Disabilities to Register to Vote at Residences.

- Requires the EAC (subject to the availability of appropriations) to make grants to states to conduct pilot programs to allow individuals with disabilities to use electronic means (including the Internet and telephones utilizing assistive devices) to register to vote and to request and receive absentee ballots in a manner which permits the individuals to do so privately and independently at their own residences.
- States must apply to the EAC to receive a pilot program grant. States receiving a grant must submit a report to the EAC on the pilot programs carried out with the grant with respect to elections during that year.

GAO Report on Voting Access for Individuals with Disabilities

- Requires GAO to conduct an analysis after each election that covers the following topics
    - polling places located in houses of worship or other facilities that may be exempt from accessibility requirements under the ADA, including efforts to overcome accessibility challenges posed by the facilities and the extent to which the facilities are used as polling places;
    - assistance provided by the EAC, DOJ, and other federal agencies to help election officials improve voting access for individuals with disabilities;
    - the extent to which accessible voting machines at a polling place are located in places that are difficult to access; malfunction; or fail to provide sufficient privacy to ensure that the ballot of the individual cannot be seen by another individual.
    - the process by which federal, state, and local governments track compliance with accessibility requirements related to voting access;
    - the extent to which poll workers receive training on how to assist individuals with disabilities;
    - the extent and effectiveness of training provided to poll workers on the operation of accessible voting machines;
    - the extent to which individuals with a developmental or psychiatric disability experience greater barriers to voting, and whether poll worker training adequately addresses the needs of such individuals;
    - the extent to which state or local governments employ, or attempt to employ, individuals with disabilities to work at polling sites.
- GAO must submit report a report to Congress after each election that contains the above analysis and recommendations to promote the use of best practices used by state and local officials to address barriers to accessibility and privacy concerns for individuals with disabilities in elections.

C. Prohibiting Voter Caging

- The term "Voter Caging Document" means a non-forwardable document, sent to a registered voter or applicant and returned to the sender or a third party as undeliverable, or, any document, sent to a registered voter or applicant, with instructions to return to the sender but not returned, despite an attempt to deliver the document to a registered voter or applicant, unless at least two Federal election cycles have passed.
- The term "voter caging list" means a list of individuals compiled from voter caging documents.
- The term "unverified match list" means any list produced by matching the information of registered voters or applicants to a list of individuals who are ineligible to vote because of death, conviction, change of address, or otherwise, unless one of the pieces of information matched includes a signature, photograph, or unique identifying number ensuring that the information from each source refers to the same individual.

Prohibition Against Voter Caging

- No state or local election official may prevent an individual from registering or voting, or permit a challenge to an individual's eligibility, based on a voter caging document or list, an unverified match list, an immaterial error or omission on voting materials, or any other evidence designate by the EAC, unless the official has other independent evidence of the individual's ineligibility to vote.

Challenges by Persons Other Than Election Officials

- No person other than a state or local election official may challenge an individual's ability to register and vote unless the challenge is supported by personal knowledge of the grounds for ineligibility which is documented in writing and subject to oath or attestation under penalty of perjury that the challenger has a good faith factual belief that the individual is ineligible to register or vote, except a challenge based on race, ethnicity, or national origin may not be considered to have a good faith basis.

Prohibition on Challenges On or Near Date of Election

- No person, other than a state or local election official, shall be permitted to challenge an individual's eligibility to vote in an election for federal office on Election Day, or to challenge an individual's eligibility to register to vote in an election for federal office or to vote in an election for federal office less than 10 days before the election unless the individual registered to vote less than 20 days before the election.

Penalties

- Anyone who knowingly challenges the eligibility of an individual to register to vote or causes the individual to be challenged in violation of the above provisions with the intent that the voter be disqualified will be fined, imprisoned for up to 1 year, or both.

EAC Best Practices to Prevent Voter Caging

No later than 180 days after the enactment, the EAC must develop and publish recommendations for best practices to deter and prevent violations of voter caging prohibitions, including practices to provide for the posting of relevant information at polling places and voter registration agencies, the training of poll workers and election officials, and relevant educational measures.

D. Prohibiting Deceptive Practices and Preventing Voter Intimidation

False Election Statements

- Prohibits any person within 60 days of an election from communicating, by any means, or producing with the intent to communicate, certain election related information that the person knows to be materially false and with the intent to impede or prevent another person from voting. Information prohibited by this provision includes false information regarding:
    - the time, place, or manner of an election;
    - the qualifications for or restrictions on voter eligibility for an election, including any criminal penalties associated with voting, or information regarding a voter's registration status or eligibility.

False Statements Regarding Public Endorsements

- Prohibits any person within 60 days of an election from communicating, by any means, information about an endorsement that the person knows to be materially false and with the intent to impede or person from voting. Information is materially false if it falsely claims that person, political party, or organization has endorsed a specific candidate.

Hindering, Interfering With, or Preventing Registration and Voting

- Prohibits any person from intentionally hindering, interfering with, or preventing another person from voting, registering to vote, or aiding another person to vote or register in an election.
- A violation of the above provision is punishable by a fine of up to $100,000, 5 years imprisonment, or both.

Private Right of Action

- Authorizes a person aggrieved by a violation of the above provisions to institute a civil action for preventive relief.

Voter Intimidation Penalty

- The penalty for voter intimidation in Title 18 of the U.S. Code (crimes and criminal procedure) is amended to provide for a penalty of up to 5 years imprisonment or a fine of up to $100,000.

Sentencing Guidelines

- No later than 180 days after enactment of the Act, the US Sentencing Commission must review and if appropriate amend the federal sentencing guidelines applicable to persons convicted of any offense under the above provisions.

Corrective Action

- If the Attorney General receives a credible report that materially false information has been or is being communicated in violation of the above prohibitions against false statements, and the Attorney General determines that state and local election officials have not taken adequate steps to promptly communicate accurate information to correct the materially false information, the Attorney General communicate to the public, by any means, accurate information designed to correct the materially false information. The communication must be accurate and objective and consist of only the information necessary to correct the false information.
- No later than 180 after the date of enactment of this Act, the Attorney General must publish written procedures and standards for determining when and how corrective action will be taken. The procedures and standards must include appropriate deadlines. The Attorney General must consult with the EAC, state and local election officials, civil right organization, and other stakeholder groups in developing the procedures and standards.

Authorization of Appropriations

- Authorizes to be appropriated to the Attorney General such sums as may be necessary to carry out the above provision.

Reports to Congress

- No later than 180 days after each general election the Attorney General must submit to Congress a report compiling all allegations received by the Attorney General of deceptive practices. Each report must address several criteria, including a description of the allegations, the status of each investigation, and the corrective action taken.
- The report must be made public on the day it is submitted.

E. Democracy Restoration

Voting Rights of Citizens

- Prohibits denying a US citizen in a correctional facility the right to vote in federal elections because the individual has been convicted of a criminal offense, unless the individual is serving a felony sentence at the time of the election.

Enforcement

- A violation may be reported to the chief state election official. If the violation is not corrected within 90 days (or within 20 days if the violation occurred within 120 days before a federal election) the individual may bring a civil action to obtain declaratory or injunctive relief. If the violation occurs within 30 days before a federal election, the individual is not required to give notice to the chief state election official before bringing a civil action.

State Notification Requirements

- On the date that an individual convicted of a felony is either released from custody or sentenced to probation, the state (if a violation of state law) must notify the individual of the right to register and vote.

Federal Notification Requirements

- On the date that an individual convicted of a felony under federal law is sentenced to probation, the Office of Probation and Pretrial Services must notify the individual of the right to register and vote.
- During the 6-month period before an individual convicted of a felony under federal law is released, the Bureau of Prisons must notify the individual of the right to register and vote.
- If an individual is convicted of a misdemeanor under federal, the above notification must be given on the date the individual is sentenced.

Use of Federal Prison Funds

- No state or local government may receive or use federal prison funds to construct or improve a jail or other incarceration facility unless it has implemented a program for notifying incarcerated individuals of their right to register and vote upon release from incarceration.

Effective Date

The above requirements apply to all federal election held after enactment.

F. Promoting Accuracy, Integrity, and Security Through Voter Verified Permanent Paper Ballot

Voter Verified Paper Ballot Requirement

- All voting systems must use voter verified paper ballots that are marked by the voter or a ballot marking device and counted by hand, optical scanner, or other counting device. The voting system must provide the voter with the opportunity to inspect, verify, and correct any errors on the ballot before it is cast and counted.
- The voting system must not preserve the paper ballot in any way that makes it possible after the vote is cast to associate a voter with the record of the voter's vote without the voter's consent.
- The paper ballots must be preserved and counted by hand in any recount or audit. If there is a discrepancy between the electronic vote tally and the paper ballot hand count tally, the hand count tally will be the correct record of votes cast.
- If any audit, recount, or election contest shows clear and convincing evidence that a sufficient number of paper ballots have been compromised that could change the results of the election, the determination of the appropriate remedy must be made in accordance with state law, except that the electronic tally must not be used as the exclusive basis for determining the official certified result.
- All paper ballots must be printed on durable paper. Paper is durable if it can withstand multiple counts and recounts and still retain the information printed on them for a 22-month retention period.

- All paper ballots completed through a ballot marking device must be clearly readable by the voter without assistance and by an optical character recognition device or other device equipped for individuals with disabilities.
- Beginning January 1, 2021, all paper ballots must be printed on recycled paper. Paper ballots must be printed on paper manufactured in the United States.

Study and Report on Optimal Ballot Design

- The EAC must conduct a study of the best ways to design ballots, including paper ballots and electronic or digital ballots, to minimize confusion and user errors. The EAC must report to Congress on the study.

Accessible Voting Machines

- Individuals with disabilities must be given an equivalent opportunity to vote, including privacy and independence, in a manner that produces a voter verified paper ballot as for other voters.
- HAVA voting system requirements for individuals with disabilities may be met through the use of at least one voting system at each polling place that:
    - is equipped with nonvisual and enhanced visual accessibility for the blind and visually impaired, and nonmanual and enhanced manual accessibility for the mobility and dexterity impaired;
    - allows the voter to privately and independently verify the paper ballot through the accessible presentation of the same printed or marked vote selections that will be used for vote counting and auditing; and
    - allows the voter to verify and cast the paper ballot without requiring the voter to manually handle the paper ballot.

Study and Report on Accessible Paper Ballot Verification

- The Director of the National Science Foundation must make grants available to at least 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot verification for individuals with disabilities, voters whose primary language is not English, and voters with difficulties in literacy.
- An entity is eligible to receive a grant if it submits to the NSF an application that certifies that it will investigate enhanced methods or devices and complete the activities by December 31, 2020.
- Any technology developed with the grants must be considered non-proprietary and be made publicly available.
- $5 million is authorized to be appropriated to the National Science Foundation.

Implementation Deadlines

- The paper ballot voting system requirements apply beginning with elections held in 2022, except that states voting systems that use a paper record printer attached to a DRE or other voting system that uses or produces a verifiable paper record of the vote may delay implementation of paper ballot voting systems until the 2024 election.
- Jurisdictions which delay the implementation of paper ballot voting systems until 2024 must provide voters with the opportunity to mark and cast a paper ballot. Election officials must ensure (to the greatest extent practicable) that the waiting period for individuals to cast a paper ballot is the lesser of 30 minutes or the average wait period of a voter who does not use a paper ballot. Any paper ballot cast under these provisions must be treated as a regular ballot for all purposes. Election officials must display prominent notice that paper ballots are available. The chief state election official must ensure that polling place election officials are aware of the optional paper ballot requirements.

G. Provisional Ballots

Statewide Counting of Provisional Ballots

- The appropriate election official must count each vote on a provisional ballot, regardless of the precinct or polling place at which the provisional ballot was cast within the state.
- Each state must establish uniform and nondiscriminatory standards for the issuance, handling, and counting of provisional ballots.

Effective Date

- The above provisional ballot requirements apply with respect to elections held on or after January 1, 2020.

H. Early Voting

Early Voting Requirement

- Each state must allow individuals to vote in an election during a period of consecutive days (including weekends) beginning 15 days prior to the election (or earlier at the option of the state) in the same manner as voting is allowed on Election Day.
- Each polling place for early voting must allow voting no less than ~~4~~ 10 hours on each day ~~(except Sunday may allow voting for fewer than 4 hours)~~ and have uniform hours for each day of voting~~.~~; and allow early voting to be held for some time period of time prior to 9 AM (local time) and some period of time after 5 PM (local time).
- To the greatest extent practicable, a state must ensure that each polling place which allows early voting is located within walking distance of a stop on a public transportation route.
- States must ensure that polling places which allow voting during an early voting period will be located in rural areas of the state, and ensure the polling places are located in communities which will provide the greatest opportunity for residents of rural areas to vote during the early voting period.
- The EAC must issue standards for the administration of early voting, including the nondiscriminatory geographic placement of polling places. The standards must allow states to deviate from any requirements in the case of unforeseen circumstances such as a natural disaster.
- The above early voting requirements apply with respect to elections held on or after January 1, 2020.

I. Voting by Mail

Promoting Vote by Mail

- If an individual is eligible to cast a vote in a federal election, the state may not impose any additional requirements on an individual's ability to vote by mail, except for ballot request and return deadlines and signature verification requirements.

Signature Verification

- A state may not accept and process an absentee ballot unless it verifies the signature on the ballot by comparing it with the person's signature on the official voter registration list, subject to the following due process requirements:
    - if an individual submits an absentee ballot and the appropriate election official determines that a discrepancy exists between the signature on the ballot and the signature of the individual on the official list of registered voters the election official, prior to making a final determination as to the validity of the ballot, must make a good faith effort to immediately notify the individual by mail, telephone, and (if available) electronic mail that:

        - a discrepancy exists between the signature on such ballot and the signature of the individual on the voter registration list;
        - the individual may provide the official with information to cure the discrepancy, either in person, by telephone, or by electronic methods;
        - and if such discrepancy is not cured 5 prior to the expiration of the 7-day period which begins on the date of the election, the ballot will not be counted.
    - An election official may not make a determination that a discrepancy exists between the signature on an absentee ballot and the signature of the individual who submits the ballot on the official list of registered voters unless at least 2 election officials make the determination and each official who makes the determination has received training in procedures used to verify signatures.

- No later than 120 days after the end of a federal election cycle, each chief state election official must submit to Congress a report that includes the number of ballots invalidated due to a discrepancy; a description of attempts to contact voters to provide notice; a description of the cure process developed by such State pursuant to this subsection, including the number of ballots determined valid as a result of such process

Deadline for Absentee Ballot Materials

- If an individual request to vote by absentee ballot, the appropriate state or local official must ensure that the ballot and related materials are transmitted no later than 2 weeks before the election, or, if a state imposes a request deadline that is than 2 weeks before the election, as expeditiously as possible, before the date of the election.

Accessibility for Individuals with Disabilities

- The state must ensure that all absentee ballots and related materials are accessible to individuals with disabilities in a manner that provides the same opportunity for access and participation (including with privacy and independence) as for other voters.

Payment of Postage on Ballot

- Consistent with regulations of the US Postal Service, the state or the unit of local government responsible for the administration of an election for federal office must prepay the postage on any ballot in the election which is cast by mail.

Deadline for Acceptance of Mailed Ballots

- If a ballot submitted by an individual by mail is postmarked on or before the date of the election, the state may not refuse to accept or process the ballot on the grounds that the individual did not meet a deadline for returning the ballot to the appropriate election official.

Permitting Ballot Return to Polling Place

- States must permit an individual to whom an absentee ballot was provided to cast the ballot on Election Day by delivering the ballot to a polling place.

Development of Biometric Verification

- NIST in consultation with the EAC must develop standards for the use of biometric methods which could be used voluntarily in place of the signature verification requirements of HAVA for purposes of verifying the identification of an individual voting by absentee ballot. NIST must solicit comments from the public in the development of standards. No later than one year after enactment NIST must publish the standards.

No Impact on UOCAVA

- None of the above provisions affect the treatment of UOCAVA ballots.

Effective Date

- The above requirements apply with respect to elections held on or after January 1st, 2020.

J. Absent Uniformed Services Voters and Overseas Voters

Pre-Election Reporting

- No later than 55 days before the election, each state must submit a report to the DOJ, the EAC, and the DOD certifying that absentee ballots will be available for transmission to UOCAVA voters no later than 45 days before the election. The state must make the report publicly available the same day. The report must be in a form specified by the Attorney General and the EAC and must require the state to certify specific information about ballot availability from each unit of local government that will administer the election.
- No later than 43 days before the election, states must submit a report to the DOJ, EAC, and the DOD certifying that whether all absentee ballots were transmitted to UOCAVA voters no later than 45 days before the election. The state must make the report publicly available the same day. The report must be in a form specified by the Attorney General and the EAC and must require the state to certify specific information about ballot transmission, including the total number of ballot requests received and ballots transmitted from each unit of local government that administers the election.

Post-Election Reporting

- No later than 90 days after the election, each state must submit a report to the DOJ, EAC, and DOJ on the combined number of absentee ballots transmitted to UOCAVA voters, and the combined number of ballots returned by UOCAVA voters and cast. The state must make the report publicly available the same day.

DOJ Enforcement and Penalties

- The DOJ may bring a civil action in district court for declaratory or injunctive relief. If a court finds that a state violated provisions of UOCAVA, it may, to vindicate the public interest, assess a penalty against the state of up to $110,000 for a first violation, and up to $220,000 for each subsequent violation.

Report to Congress

- No later than December 31st of each year, the DOJ must submit a report to Congress on any civil actions brought under this provision.

Private Right of Action

- A person aggrieved by UOCAVA may bring a civil action for declaratory or injunctive relief.

State as Defendant

- In any civil action brought under the above provisions, the only necessary party is the state, and it is no defense to any action that a local election official or unit of government is not named as a defendant, regardless of whether a state has exercised authority under the MOVE Act to delegate relevant duties to another jurisdiction.

Effective Date

The above enforcement and litigation provisions apply with respect to any violations alleged to have occurred on or after the date of the enactment of the Act.

Waiver Provision Repealed

- The waiver provision in the MOVE Act is repealed.

Express Delivery Requirement

- If a state fails to transmit an absentee ballot to a UOCAVCA no later than 45 days before the election, the state must transmit the ballot to the voter by express delivery, or, transmit the ballot electronically, if the voter has designated this option.
- If a state transmits a ballot to a UOCAVA voter less than 40 days before an election, the state must enable return of the ballot by express delivery, however, with regard to absentee ballots for uniformed services voters, the state may satisfy the requirement by notifying the voter of the DOD express delivery procedures under the MOVE Act.
- The state is responsible for the payment of the costs associated with the use of express delivery for the transmittal of ballots.

Clarification of Weekend Mailing Deadlines

- When the 45th day before an election falls on a weekend or holiday, absentee ballots must be sent no later than the most recent weekday which precedes 45th day and is not a legal public holiday, but only if the request is received by at least such most recent weekday.
- The above provision applies with respect to voter registration and absentee ballot applications submitted to state or local election officials on or after the date of enactment.

Use of FPCA for Subsequent Elections

- A voter may request that an FPCA be considered an application for absentee ballots for each subsequent federal election in the state through the next regularly scheduled general election. This provision does not apply with regard to any election held after the vote notifies the state that the voter no longer wishes to be registered to vote or the state determines that the voter is no longer eligible in the state.

Prohibiting Refusal of Early Submissions

- A state must accept and process a valid voter registration/absentee ballot application submitted by either a uniformed services voter or overseas voter at any time during the calendar year in which an election for federal office is held. This section applies with respect to applications submitted on or after the date the Act is enacted.

Effective Date

- The above requirements apply with respect to elections occurring on or after January 1, 2019.

Extending Guarantee of Voting Residency to Military Personnel Family

- Amends UOCAVA to require that for purposes of voting in any federal, state, or local office, a spouse or dependent of an individual who is an absent uniformed services voter must not, solely because of the absence and without regard to whether or not such spouse or dependent is accompanying that individual: be deemed to have lost a residence or domicile in that state, without regard to whether or not that individual intends to return to that state; be deemed to have acquired a residence or domicile in any other state; or be deemed to have become a resident in or a resident of any other state.

K. Poll Worker Recruitment and Training

Grants for Poll Worker Training and Recruitment

- The EAC must make grants available to each state (subject to the availability of appropriations) for recruiting and training individuals to serve as poll workers. In carrying out activities with a grant, the recipient must use the poll worker practices manual prepared by the EAC and develop training programs with assistance from experts in adult learning.

- The EAC must ensure that the manual provides training in methods that will enable poll workers to provide access and delivery of services in a culturally competent manner to all voters who use their services, including those with limited English proficiency, diverse cultural and ethnic backgrounds, disabilities, and regardless of gender, sexual orientation, or gender identity.
- States seeking a grant must submit an application to the EAC describing the activities to be carried out providing on the use of the funds and assurances that the state will provide the EAC with relevant recruitment and training data.
- The amount of a grant to a state must be equal to the product of the aggregate amount made available for grants to states and the voting age population percentage for the state.

Reporting

- No later than 6 months after a grant is made, each recipient must submit a report to the EAC on the activities conducted with the grant funds.
- No later than 1 year after a grant is made, the EAC must submit a report to Congress on the grant activities carried out by recipients, and any recommendations.

Funding

- Any amount appropriated to carry out the above provisions must remain available without fiscal year limitation.
- Of the amounts appropriated for any fiscal year, no more than 3 percent must be available for EAC administrative expenses.

L. Enhancement of Enforcement

Filing of Complaints

- A person aggrieved by Title III of HAVA (election technology and administration requirements) may file a written, notarized complaint with the Attorney General describing the violation and requesting appropriate action. The Attorney General must provide a copy of the complaint to the entity responsible for administering the state based administrative complaint procedures under HAVA.
- The Attorney General must respond to each complaint within the same deadlines that apply to state based administrative complaint procedures under HAVA.

Private Right of Action

- Any person who files a complaint under the previous section (including for purposes of enforcing the individual's right to a voter verified paper ballot) may file an action to enforce the uniform and nondiscriminatory election technology and administration requirements of Title III.

Effective Date

- The above requirements apply with respect to violations that occur with respect to federal elections beginning in 2020.

M. Federal Election Integrity

Prohibition on Chief Election Official Campaign Activity

- Chief state election administration officials are prohibited from taking an active part in political management, or in a political campaign with respect to any election for federal office over which the official has supervisory authority.

- A chief state election official is defined as the highest state official with responsibility for administering federal election under state law.

Prohibited Activities

- Prohibited activities with regard to taking an active part in political management or in a political campaign includes:
    - serving as a member of an authorized committee of a candidate for federal office;
    - using official authority to interfere with or affect the results of an election; and
    - soliciting, accepting, or receiving a contribution from anyone on behalf of a candidate for federal office

Exception

- The prohibition does not apply to any chief state election official with respect to a federal election in which the official or an immediate family member is an official candidate, but only if the official recuses himself or herself from all official responsibilities for the administration of that election and the official who assumes responsibility for supervising the administration of the election does not report directly to the official.

Effective Date

- The above requirements apply with respect to federal elections held after December 2019.

N. Promoting Voter Access Through Election Administration Improvements

1. Promoting Voter Access

Universities as Voter Registration Agencies

- Institution of higher education are designated as voter registration agencies under NVRA if they have a program participation agreement in effect with the Secretary of Education, other than an institution which is treated as a contributing agency under the Automatic Voter Registration Act of 2019.

Responsibilities of Institutions of Higher Education under Higher Education Act

- Amends section 487(a)(23) of the Higher Education Act of 1965 (regarding good faith voter registration efforts for institutions located in states that are not exempt from NVRA) to require the following:
    - The institution must ensure that an appropriate staff person or office is designated publicly as a 'Campus Vote Coordinator';
    - Not fewer than twice during each calendar year (beginning with 2020), the Campus Vote Coordinator must transmit electronically to each student enrolled in the institution (including students enrolled in distance education programs) a message containing the following information: information on the location of polling places in the jurisdiction in which the institution is located, together with information on available methods of transportation to and from such polling places; a referral to a government-affiliated website or online platform which provides centralized voter registration information for all states, including access to applicable voter registration forms and information to assist individuals who are not registered to vote in registering to vote; any additional voter registration and voting information the Coordinator considers appropriate, in consultation with the appropriate state election official.

- Not fewer than twice during each calendar year, the Campus Vote Coordinator must transmit the message not fewer than 30 days prior to the deadline for registering to vote for any election for federal, state, or local office in the state.

- If the institution in its normal course of operations requests each student registering for enrollment in a course of study, including students registering for enrollment in a program of distance education, to affirm whether or not the student is a United States citizen, the institution will comply with the applicable requirements for a contributing agency under the Automatic Voter Registration Act. If the institution does not meet these criteria, the institution will comply with the requirements for a voter registration agency in the state.
- The above provisions apply only with respect to an institution located in a state which is not exempt from NVRA.
- The above requirements apply respect to elections held on or after January 1, 2020.

Grants to Institutions Demonstrating Excellence in Student Voter Registration

- The Secretary of Education may award competitive grants to institutions of higher education that the Secretary determines have demonstrated excellence in registering students to vote in elections for public office beyond meeting the minimum requirements under applicable laws. An institution of higher education is eligible to receive a grant if the institution submits to the Secretary of Education an application containing such information and assurances as the Secretary may require to make the determination, including information and assurances that the institution carried out activities to promote voter registration by students, such as sponsoring large on-campus voter mobilization efforts; engaging the surrounding community in nonpartisan voter registration and get out the vote efforts; creating a website for students with centralized information about voter registration and election dates; inviting candidates to speak on campus; offering rides to students to the polls to increase voter education, registration, and mobilization.
- Authorizes such sums as may be necessary for FY 2020 and succeeding fiscal years.

Polling Place Notification Requirements

- If a state assigned a registered voter to a new polling place, the state must notify the individual of the location of the new polling place no later than 7 days before the election, or if the state makes the assignment less than 7 days before the election and the individual appears at the previous polling place, the state must make every effort to enable the individual to vote on the day of the election.
- This requirement applies with respect to elections held on or after January 1, 2020.

Election Day Holiday

- For purposes of any law relating to Federal employment, the Tuesday next after the first Monday in November in 2020 and each even-numbered year thereafter must be treated in the same manner as a legal public holiday.

Use of Sworn Written Statements to Meet Voter Identification Requirements

- If a state requires that an individual present identification as a condition of receiving and casting a ballot the state must permit the individual, when voting in person, to meet the requirement by presenting the appropriate state or local election official with a sworn written statement, signed by the individual under penalty of perjury, attesting to the individual's identification and attesting that the individual is eligible to vote in the election.
- Where a person desires to vote by mail, the person must be permitted to meet the requirement by submitting the sworn written statement with the ballot.

- The EAC must develop:
    - prepare a pre-printed version of the statement which includes a blank space for an individual to provide a name and signature; for use by election official in states subject to the above provisions.
    - make copies of the pre-printed version developed by the EAC available at polling places for election officials to distribute to individuals who desire to vote in person; and
    - include a copy of the pre-printed version with each blank absentee or other ballot transmitted to an individual who desires to vote by mail.
- An individual who presents or submits a sworn written statement must be permitted to cast a regular ballot in the election in the same manner as an individual who presents identification.
- The above requirements do not apply with respect to an individual required to meet the HAVA requirements for first-time voters registering by mail.
- In states with a voter identification requirement, informational materials required to be posted at polling places under HAVA must include information on how an individual may meet the identification requirement by presenting a sworn written.
- The above requirements apply with respect to elections held on or after enactment.

Postage-Free Ballots

- Absentee ballots for any election must be carried expeditiously with postage prepaid by the state or unit of local government responsible for the administration of the election. As used in this section, the term 'absentee ballot' means any ballot transmitted by a voter by mail in an election for federal office (not including UOCAVA ballots).

Absentee Ballot Tracking Program

- An absentee ballot tracking program is a program to track and confirm the receipt of absentee ballots and make information on the receipt of the ballots available online. The information must include whether the ballot was counted, and, if not counted, the reasons why.
- A state or local election office that does not have an internet site may meet the program requirements if the official has established a toll-free telephone number that may be used to obtain the information.
- The EAC must make payments to states for costs incurred in establishing, if the state chooses, an absentee ballot tracking program, including costs incurred prior to enactment.
- In order to receive a payment a state must submit to the EAC a statement containing a certification that the State has established an absentee ballot tracking program, and a statement of the costs incurred in establishing the program.
- The amount of a payment made to a state must be equal to the costs incurred by the state in establishing the program, except that the amount may not exceed the product of the number of jurisdictions in the state responsible for operating the program, and $3,000. A state may not receive more than one payment.
- Such sums as may be necessary are authorized to be appropriated to the EAC for FY 2020 for absentee ballot tracking program payments.

Voter Information Resources

- The Attorney General must coordinate the establishment of a state-based response system for responding to voting related questions and complaints. The system must provide state specific, same day immediate assistance, including information on registering to vote, polling place hours and locations, and obtaining

absentee ballots, and assistance to individuals encountering problems with registering to vote or voting including intimidation or deceptive practices.

- The Attorney General, in consultation with state election officials, must establish a toll-free hotline through which individuals may connect directly to the state-based response system, obtain information on voting, and report information to the Attorney General on problems encountered in registering to vote or voting, including voter intimidation or suppression.
- The Attorney General must coordinate the collection of information on state and local election laws and policies, including information on the statewide voter registration lists, so that individuals who contact the hotline may receive an immediate response on that day.
- If a person contacts the hotline on Election Day with a question or complaint, the Attorney General must forward the matter to the appropriate state or local election official.
- The Attorney General must ensure the state-based response systems are developed in consultation with civil rights organization, voting rights groups, state and local election officials, and other stakeholders.
- The Attorney General must provide a telephone service that individuals with disabilities are fully able to use, and must ensure the assistance is provided in any language the state or jurisdiction must provide election materials under the Voting Rights Act.
- The Attorney General must appoint no less than 3 individuals to serve on a Voter Hotline Task Force to provide ongoing analysis and assessment of the operation of the telephone service.
- At least one member of the Task Force must be a representative of an organization promoting voting rights or civil rights with experience in operating similar telephone services or in protecting the rights of individuals to vote.
- Task Force members serve a single term of 2 years. No compensation is provided.
- No later than March 1st of each odd numbered year the Attorney General must submit a report to Congress on the operation of the telephone service.
- Such sums as are necessary are authorized to be appropriated to the Attorney General for Fiscal Year 2019 and each succeeding fiscal year. No less than 15% of the funding must be used for public outreach activities.

Limiting Variations on Number and Hours of Polling Places

- Requires each state to establish polling place hours for all polling places in the state so that the polling place with the greatest number of hours of operation is not in operation more than 2 hours longer than the polling place with the fewest number of operating hours.
- The above provision does not apply to the extent the state establishes variations in polling places hours on the basis of the overall population or the voting age population (as the state may select) of the unit of local government in which the polling places are located.
- Provides an exception to the polling place hours requirement for polling places whose hours of operation are established, in accordance with state law, by the unit of local government in which the polling place is located, or which is required pursuant to an order by a court to extend its hours of operation.

2. Improvements in the Operation of the EAC

Reauthorization of the EAC

Appropriations are authorized for FY 2019 and each succeeding fiscal year for the EAC to carry out HAVA.

Requiring State Participation in Post-Election Surveys

- Each state must provide the EAC with the information required for purposes of conducting any post-election survey of the states with respect to election administration.
- This requirement applies with respect to the 2020 election and succeeding elections.

Recommendations to Improve the EAC

- No later than December 31,2019, the EAC must shall carry out an assessment of the security and effectiveness of the its information technology systems, including the cybersecurity of the systems.
- The EAC must carry out a review of the effectiveness and efficiency of the state-based administrative complaint procedures under HAVA. No later than December 31, 2019, the EAC must submit to Congress a report on the review that includes recommendations the EAC considers appropriate to streamline and improve the procedures.
- Repeals Section 205(e) of HAVA which provides an exemption to the EAC for certain contracting requirements. This provision goes into effect with respect to contracts entered into by the EAC on or after the date of enactment.

Election Integrity

A. Findings

Expresses the findings of Congress on the following topics:

- Findings Reaffirming Commitment of Congress to Restore the Voting Rights Act
- Findings Relating to Native American Voting Rights
- Findings Relating to District of Columbia Statehood
- Findings Relating to Territorial Voting Rights

B. Saving Voters from Voter Purging

Conditions for Removal of Voters from List of Registered Voters

- A state may not remove any registrant from the official list of voters eligible to vote in elections for Federal office in the State unless the State verifies, on the basis of objective and reliable evidence, that the registrant is ineligible to vote in such elections on any of the grounds described in applicable provisions in NVRA.
- The following factors, or any combination, must not be treated as objective and reliable evidence of a registrant's ineligibility to vote:
    - the failure of the registrant to vote in any election;
    - the failure of the registrant to respond to any notice sent under the applicable provisions of NVRA, unless the notice has been returned as undeliverable;
    - the failure of the registrant to take any other action with respect to voting in any election or with respect to the registrant's status as a registrant.
- No later than 48 hours after a state removes the name of a registrant from the official list of eligible voters for any reason (other than the death of the registrant), the state shall send notice of the removal to the former registrant, and must include in the notice the grounds for the removal and information on how the former registrant may contest the removal or be reinstated, including a telephone number for the

appropriate election official. and how to contest the removal or be reinstated, in cluding a contact phone number.

- The above paragraph does not apply in the case of a registrant who sends written confirmation to the state that the registrant is no longer eligible to vote in the registrar's jurisdiction in which the registrant was registered or who is removed from the official list of eligible voters by reason of the death of the registrant.
- No later than 48 hours after conducting any general program to remove the names of ineligible voters from the official list of eligible voters the state shall disseminate a public notice through such methods as may be reasonable to reach the general public (including by publishing the notice in a newspaper of wide circulation or posting the notice on the websites of the appropriate election official that list maintenance is taking place and that registrants should check their registration status to ensure no errors or mistakes have been made. The state must ensure that the public notice disseminated under this paragraph is in a format that is reasonably convenient and accessible to voters with disabilities, including voters who have low vision or are blind.
- A state may not transmit a removal notice to a registrant unless the state obtains objective and reliable evidence (in accordance with the above standards for such evidence) that the registrant has changed residence to a place outside the registrar's jurisdiction in which the registrant is registered.
- The above requirements are effective on the date of enactment.

Election Security

A. Financial Support Election Infrastructure

1. Voting System Security Improvement Grants

Grants for Paper Ballot Voting Systems and Election Security Improvements

- The EAC must make grants to states for replacing voting systems that do not meet the requirements of the Voter Confidence and Increased Accessibility Act and the voluntary voting system guidelines, and to carry out voting system security improvements (described below), and to implement and model best practices for ballot design, ballot instructions, and the testing of ballots. The provisions must be implemented by the 2020 election.
- The EAC must determine the appropriate grant amount, except that it may not be less than the product of $1 and the average of the number of individuals who cast votes in any of the two most recent regularly scheduled general elections for Federal office in the state.
- The EAC must make pro rata reductions as necessary to ensure the entire amount appropriated is distributed to states.
- If the amount of funds appropriated exceeds the amount necessary to meet the grant requirements, the EAC must consider the following in making a determination to award remaining funds to a state:
    - The record of the state in carrying out the following:
        - providing voting machines that are less than 10 years old;
        - implementing strong chain of custody procedures for the physical security of voting equipment and paper records;
        - conducting pre-election testing on every voting machine and ensuring that paper ballots are available wherever electronic machines are used;

- maintaining offline backups of voter registration lists;
- providing a secure voter registration database that logs requests submitted to the database;
- publishing and enforcing a policy detailing use limitations and security safeguards to protect the personal information of voters in the voter registration process;
- providing a secure processes and procedures for reporting vote tallies;
- providing a secure platform for disseminating vote totals;
- evidence of established conditions of innovation and reform in providing voting system security and the proposed plan of the State for implementing additional conditions;
- evidence of collaboration between relevant stakeholders;
- the plan of the State to conduct a rigorous evaluation of the effectiveness of the activities carried out with the grant.

- To the greatest extent practicable, an eligible state which receives a grant to replace a voting system must ensure that the replacement system is capable of administering a system of ranked choice voting under which each voter shall rank the candidates for the office in the order of the voter's preference.
- Voting system security improvements for purposes of the receiving grant funds are any of the following:
    - the acquisition of goods and services from qualified election infrastructure vendors;
    - cyber and risk mitigation training;
    - a security risk and vulnerability assessment of the state's election infrastructure carried out by a provider of cybersecurity services under a contract entered into between the chief state election official and the provider;
    - the maintenance of election infrastructure, including addressing risks and vulnerabilities;
    - providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure;
    - enhancing the cybersecurity and operations of the information technology infrastructure;
    - enhancing the cybersecurity of voter registration systems;
- For the purposes of voting system security improvements, a "qualified election infrastructure vendor" is any person who provides, supports, or maintains infrastructure on behalf of a state, local government, or election agency that meet requirements established by the EAC and DHS, which must include the following criteria:
    - the vendor must be owned and controlled by a citizen or permanent resident of the US;
    - the vendor must disclose to the EAC and DHS, and the relevant chief state election official any sourcing outside the US for parts of the election infrastructure;
    - the vendor agrees to ensure that the election infrastructure will be developed and maintained in a manner consistent with cybersecurity best practices issued by the TGDC;
    - the vendor agrees to maintain its information technology infrastructure in a manner consistent with the cybersecurity best practices provided by the EAC and DHS;
    - the vendor agrees to meet the requirements for reporting any known or suspected cybersecurity incidents involving any of the goods and services provided by the vendor;

- the vendor agrees to permit independent testing by the EAC and DHS of the goods and services provided.

- A vendor meets the relevant reporting requirements if, upon becoming aware of the possibility that an election cybersecurity incident has occurred involving any of the goods and services provided pursuant to the grant:
    - the vendor promptly assesses whether or not such an incident occurred and submits the required notification to the EAC and DHS of the assessment as soon as practicable, but no later than 3 days after the vendor first becomes aware of the possibility that the incident occurred;
    - if the incident involves goods or services provided to an election agency, the vendor submits a notification meeting the applicable requirements to the agency as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred), and cooperates with the agency in providing any other nec1essary notifications relating to the incident; and
    - the vendor provides all necessary updates to any notification submitted as required;
- Each required notification from a vendor must contain the following information with respect to any election cybersecurity incident covered by the notification:
    - the date, time, and time zone when the election cybersecurity incident began, if known;
    - the date, time, and time zone when the election cybersecurity incident was detected;
    - the date, time, and duration of the election cybersecurity incident;
    - the circumstances of the election cybersecurity incident, including the specific election infrastructure systems believed to have been accessed and information acquired, if any;
    - any planned and implemented technical measures to respond to and recover from the incident;
    - in the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.
- a state is eligible to receive a grant if it submits to the EAC an application describing how it will use the grant to carry out the activities and a certification not later than 5 years after receiving the grant the state will carry out risk-limiting audits.
- Not later than 90 days after the end of each fiscal year, the EAC must submit a report to the appropriate congressional committees on the activities carried out with the grant funds.
- Authorizes $1 billion for FY 2019 and $175 million for FY 2020, 2022, 2024, and 2026 for the voting system security improvement grants.

<u>DHS Membership on EAC Board of Advisors and TGDC</u>

- Expands the Board of Advisors and TGDC membership to include a representative from DHS.

<u>EAC Studies</u>

- Requires the EAC to consult with DHS on periodic studies, as appropriate.
- Requires that the goal of EAC studies include promoting election methods that are secure against attempts to undermine the integrity of election systems by cyber or other means.

<u>Use of Requirements Payments</u>

- Allows states to use a requirements payment to carry out any of the following activities:

- cyber and risk mitigation training;
- providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure;
- enhancing the cybersecurity and operations of the information technology infrastructure;
- enhancing the security of voter registration databases

State Plan Description Update

- Requires that the state plan description of how the state will use requirements payments to improve the administration of elections include the protection of election infrastructure.

Composition of State Plan Committee

- Updates the composition of the committee responsible for developing the state plan to require the membership be a representative group of individuals from the state's counties, cities, towns, and Indian tribes, and represent the needs of rural as well as urban areas of the state.

Protection of Voter Registration List

- Requires that the technology measures for securing the voter registration list include measures to prevent and deter cybersecurity incidents, as identified by the EAC, DHS, and the TGDC.

2. Grants for Risk-Limiting Audits of Results of Elections

Grants for Risk-Limiting Audits

- Requires that the make grants to states to conduct risk limiting audits with respect to the 2020 election and each succeeding election
- A risk-limiting audit is a post-election process:
  - conducted in accordance with rules and procedures established by the chief state election official of the state which meet the applicable requirements;
  - under which, if the reported outcome of the election is incorrect, there is at least a predetermined percentage chance that the audit will replace the incorrect outcome with the correct outcome as determined by a full, hand-to-eye tabulation of all votes validly cast in that election that ascertains voter intent manually and directly from voter verifiable paper records.

Risk-Limiting Audit Requirements

- Rules and procedures established for conducting a risk-limiting audit must include the following elements:
  - rules for ensuring the security of ballots and documenting that prescribed procedures were followed;
  - rules and procedures for ensuring the accuracy of ballot manifests produced by election agencies;
  - rules and procedures for governing the format of ballot manifests, cast vote records, and other data involved in the audit;
  - methods to ensure that any cast vote records used in the audit are those used by the voting system to tally the election results sent to the chief state election official and made public;
  - procedures for the random selection of ballots to be inspected manually during each audit;

- rules for the calculations and other methods to be used in the audit and to determine whether and when the audit of an election is complete;
- procedures and requirements for testing any software used to conduct risk-limiting audits.

- The term "ballot manifest" means a record maintained by each election agency that meets each of the following requirements:
  - the record is created without reliance on any part of the voting system used to tabulate votes;
  - the record functions as a sampling frame for conducting a risk-limiting audit;
  - the record contains the following information with respect to the ballots cast and counted in the election:
    - the total number of ballots cast and counted by the agency (including undervotes, overvotes, and other invalid votes)
    - the total number of ballots cast in each election administered by the agency (including undervotes, overvotes, and other invalid votes)
    - A precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.
- The term "incorrect outcome" means an outcome that differs from the outcome that would be determined by a full tabulation of all votes validly cast in the election, determining voter intent manually, directly from voter-verifiable paper records.
- The term "outcome" means the winner of an election, whether a candidate or a position.
- The term "reported outcome" means the outcome of an election which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.

<u>Eligibility for Risk-Limiting Audit Grant</u>

- A state is eligible to receive a grant by submitting an application to the EAC that includes:
  - A certification that, no later than 5 years after receiving the grant, the state will conduct risk limiting audits of the results of elections for federal office;
  - a certification that, no later than one year after the date of enactment, the chief state election official of the state has established or will establish the rules and procedures for conducting the audits which meet the requirements;
  - a certification that the audit will be completed no later than the date on which the state certifies the results of the election;
  - a certification that, after completing the audit, the state will publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly;
  - a certification that, if a risk-limiting audit leads to a full manual tally of an election, state law requires that the state or election agency use the results of the full manual tally as the official results of the election

<u>Authorization of Appropriations</u>

- Authorizes to be appropriated for risk limiting audit grants $20 million for fiscal year 2019.

GAO Analysis

- No later than 6 months after the first election for federal office held after grants are first awarded to states for conducting risk-limiting GAO must conduct an analysis of the extent to which the audits have improved the administration of such and the security of election infrastructure.

3. Election Infrastructure Innovation Grant Program

Competitive Grant Program

- DHS, in coordination with the EAC and in consultation with the NSF must establish a competitive grant program to award grants to eligible entities, on a competitive basis, for purposes of research and development that are determined to have the potential to significantly to improve the security (including cybersecurity), quality, reliability, accuracy, accessibility, and affordability of election infrastructure.
- No later than 90 days after the conclusion of each fiscal year for which grants are awarded DHS must submit a report to Congress describing the grants and analyzing the impact, if any, of the grants on the security and operation of election infrastructure.
- Authorizes to be appropriated to DHS ~~$6,250,000~~ $20,000,000 for each of fiscal years ~~2018~~ 2019 through ~~2026~~2027.
- An "eligible entity" for purposes of the grant means:
    - an institution of higher education
    - an organization described in section 501(c)(3) of the Internal Revenue Code;
    - an organization, association, or a for-profit company, including a small business concern

B. Security Measures

Election Infrastructure Definition

- Amends the Homeland Security Act to define "election infrastructure" as storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office, as well as related information and communications technology, including voter registration databases, voting machines, electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results), and other systems used to manage the election process and to report and display election results on behalf of an election agency.

Election Infrastructure Designation

- Amends the Homeland Security Act to include election infrastructure as part of the government facilities critical infrastructure sector.

DHS Responsibilities

- Updates the DHS Secretary's responsibilities relating to intelligence and analysis to include providing timely threat information regarding election infrastructure to the chief state election official of the pertinent state.

Security clearance assistance for election officials

- Provides that in order to promote the timely sharing of information on threats to election infrastructure, DHS may:

- help expedite a security clearance for the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official;
- sponsor a security clearance for the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official; and
- facilitate the issuance of a temporary clearance to the chief state election official and other appropriate state personnel involved in the administration of elections, as designated by the chief state election official, if DHS determines classified information to be timely and relevant to the election infrastructure of the state at issue

Security risk and vulnerability assessments

- No later than 90 days after receiving a written request from a chief state election official, the DHS must, to the extent practicable, commence a security risk and vulnerability assessment on election infrastructure in the state at issue.
- If DHS determines that a security risk and vulnerability assessment cannot be commenced within 90 days, it must expeditiously notify the chief state election official who submitted the request.

Report on DHS Assistance

- No later than one year after the date of the enactment and annually thereafter through 2026, DHS must submit to Congress a report on:
  - efforts to carry out the security clearance assistance provisions during the prior year, including specific information on which states were helped, how many officials have been helped in each state, how many security clearances have been sponsored in each state, and how many temporary clearances have been issued in each state; and
  - efforts to carry out the risk and vulnerability assessment provisions during the prior year, including specific information on which states were helped, the dates on which the DHS received a request for a security risk and vulnerability assessment, the dates on which DHS commenced request, and the dates on which DHS transmitted a notification as required.

Report on Foreign Threats

- No later than 90 days after the end of each fiscal year (beginning with fiscal year 2019), DHS and the Director of National Intelligence, in coordination with the heads of appropriate offices of the Federal government, must submit a report to the appropriate congressional committees on foreign threats to elections in the US, including physical and cybersecurity threats.

Report on Assistance from States

- For the purpose of preparing the above reports DHS must solicit and consider information and comments from states and election agencies, except that providing the information and comments by a state or election agency must be voluntary and at the discretion of the state or agency.

Pre-Election Threat Assessments

- No later than 180 days before the date of each election Director of National Intelligence must submit an assessment of the full scope of threats to election infrastructure, including cybersecurity threats posed by state actors and terrorist groups, and recommendations to address or mitigate the threats, as developed by DHS and the EAC to each chief state election official and relevant Congressional committee.

- If, at any time after submitting an assessment the Director of National Intelligence determines that the assessment should be updated to reflect new information regarding the threats involved, the Director must submit a revised assessment.

C. Enhancing Protections for United States Democratic Institutions

National Strategy to Protect US Democratic Institutions

- No later than one year after the date of enactment the President must issue a national strategy to protect against cyber-attacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of US democratic institutions. The national strategy must include consideration of the following:
    - the threat of a foreign state actor, foreign terrorist organization or a domestic actor carrying out a cyber-attack, influence operation, disinformation campaign, or other activity;
    - the extent to which US democratic institutions are vulnerable to a cyber-attack, influence operation, disinformation campaign, or other activity;
    - potential consequences that could result from a successful cyber-attack, influence operation, disinformation campaign, or other activity;
    - lessons learned from other Western government institutions which were subject to a cyber-attack, influence operation, disinformation campaign, or other activity;
    - potential impacts an erosion of public trust in democratic institutions as could be associated with a successful cyber breach or other activity negatively affecting election infrastructure;
    - roles and responsibilities of DHS, EAC, other federal and non-federal entities, including election officials, and representatives of a multi-state information sharing and analysis center;
    - any findings, conclusions, and recommendations to strengthen protections for US democratic institutions that have been agreed to by a majority of members on the National Commission to Protect United States Democratic Institutions
- No later than 90 days after issuance of the national strategy, the President must issue an implementation plan for federal efforts to implement the strategy that includes:
    - strategic objectives and corresponding tasks
    - projected timelines and costs for the tasks
    - metrics to evaluate performance of the tasks

National Commission to Protect United States Democratic Institutions

- Establishes within the legislative branch the National Commission to Protect United States Democratic Institutions to counter efforts to undermine democratic institutions within the US.
- The Commission must be composed of 10 members appointed for the life of the Commission as follows:
    - one member appointed by DHS;
    - one member appointed by the EAC;
    - two members appointed by the majority leader of the Senate;
    - two members appointed by the minority leader of the Senate;
    - two members appointed by the Speaker of the House of Representatives;
    - two members appointed by the minority leader of the House of Representatives

- Individuals must be selected for appointment to the Commission solely on the basis of their professional qualifications, achievements, public stature, experience, and expertise in relevant fields, including, but not limited to cybersecurity, national security, and the U.S. Constitution.
- No later than 18 months after the date of the first meeting the Commission must submit to the President and Congress a final report containing the findings, conclusions, and recommendations to strengthen protections for democratic institutions in the US as have been agreed to by a majority of the members of the Commission.
- The Commission must terminate within 60 days of submitting the final report.

D. Promoting Cybersecurity Through Improvements in Election Administration

Compliance Testing of Existing Voting Systems

- Requires that no later than 9 months before a federal election the EAC provide for testing by an accredited laboratory of the voting system hardware and software certified for use in the most recent election, based on the most recent applicable voting system guidelines.
- If any voting system hardware of software does not meet the most recent guidelines based on the testing, it must be decertified by the EAC.
- The above requirements apply beginning with the 2020 election.

TGDC Cybersecurity Guidelines

- Requires that no later than 6 months after enactment the TGCD issue election cybersecurity guidelines including standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.

Electronic Boll Book Treatment

- Amends HAVA to treat electronic poll books as part of a voting system and defines electronic poll books as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) used to retain the list of registered voters at a polling location, or vote center, or other location at which voters cast votes in an election and to identify registered voters who are eligible to vote in an election.
- The above provision applies with respect to any requirements relating to electronic poll books on and after January 1, 2020.

Pre-Election Reports on Voting System Usage

- Requires that no later than 120 days before the date of each federal election the chief state election official submit a report to the EAC containing a detailed voting system usage plan for each jurisdiction in the state which will administer the election, including a detailed plan for the usage of electronic poll books and other equipment and components of such system.
- The above provision applies beginning with the 2020 election.

E. Preventing Election Hacking

Bug Bounty Program

- No later than 1 year after enactment of this Act, DHS must establish a program to be known as the ''Election Security Bug Bounty Program'' to improve the cybersecurity of the systems used to administer elections by facilitating and encouraging assessments by independent technical experts, in cooperation with state

and local election officials and election service providers, to identify and report election cybersecurity vulnerabilities.

- Participation in the program by state and local election officials and election service providers is voluntary.
- In developing the program DHS must solicit input from, and encourage participation by, state and local election officials.
- In establishing and carrying out the program, DHS must:
    - establish a process for state and local election officials and election service providers to voluntarily participate;
    - designate appropriate information systems to be included;
    - provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems and establish criteria to be considered eligible such compensation;
    - consult with DOJ on how to ensure that approved individuals, organizations, or companies are protected from prosecution and liability for specific activities authorized under the program;
    - consult with DOD and other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from the programs;
    - develop an expeditious process by which an individual, organization, or company can register with DHS, submit to a background check, and receive a determination as to eligibility for participation in the program;
    - engage qualified interested persons, including representatives of private entities, about the structure of the program and, to the extent practicable, establish a recurring competition for independent technical experts to assess election systems for the purpose of identifying and reporting election cybersecurity vulnerabilities
- DHS may award competitive contracts as necessary to manage the program.

Election Security Grants Advisory Committee

- Establishes an advisory committee to assist the EAC with the award of grants to states under the Act for the purpose of election security. The Committee must review grant applications received by the EAC and recommend to the EAC whether to award the grant to the applicant. In reviewing an application, the Committee must consider:
    - the record of the applicant with respect to compliance of the applicant with the requirements under subtitle A of title III and adoption of voluntary guidelines issued by the EAC under subtitle B of title III; and the goals and requirements of election security as described in title III.
    - the Committee must be composed of 15 individuals appointed by the Executive Director of the EAC with experience and expertise in election security.
- The advisory committee requirement takes effect 1 year after the date of enactment.

Use of Voting Machines Manufactured in the United States

- No later than the November 202 election each state must seek to ensure that any voting machine used in the election and in any subsequent election is manufactured in the United States.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

INVITES YOU TO ATTEND

TABLETOP THE VOTE 2019:

NATIONAL ELECTION CYBER VIRTUAL TABLETOP EXERCISE

In close partnership with
The National Association of Secretaries of State (NASS) and
The National Association of State Election Directors (NASED)

Via VTC

On June 18, 19, & 20, 2019
12:00 P.M. – 4:00 P.M. (EDT)

This event will be a series of virtual exercises focused on election cybersecurity. Identical exercises will be repeated on each of the three days and all U.S. states, territories, and the District of Columbia will be provided one VTC slot per day. Due to the limited number of VTC slots, each state will need to coordinate internally to determine the best location to conduct the exercise each day, as well as determine who will be invited to attend at each location.

An Exercise Registration Form will be emailed to state election officials by NASS or NASED and to all federal participants from the DHS Elections Security Initiative. Participants are asked to complete the form and return it to CISA at CEP@hq.dhs.gov by May 15, 2019. All VTC connections must be tested prior to the election with the DHS FEMA Video Operations Center between May 15-31, 2019. Additional details on testing will be provided on the registration form.

The Cybersecurity and Infrastructure Security Agency (CISA) is hosting the "Tabletop the Vote 2019: National Election Cyber Virtual Tabletop Exercise" on June 18, 19, & 20, 2019 via video teleconference (VTC). This three-day virtual tabletop exercise (VTTX) will assist DHS and our federal partners, state and local election officials, and private vendors in identifying best practices and areas for improvement in cyber incident planning, identification, response, and recovery.

Through tabletop simulation of a realistic scenario, exercise participants will discuss and explore potential impacts to voter confidence, voting operations, and the integrity of elections.

Proposed participants for this exercise include: all U.S. states and the District of Columbia; the Election Assistance Commission; Department of Defense; National Security Agency; U.S. Cyber Command; National Guard Bureau; Department of Justice; Federal Bureau of Investigation; Office of the Director of National Intelligence; Department of State; U.S. Attorney's Office; and the National Institute of Standards and Technology.

Questions? Please call 1-540-542-2171 or email CEP@hq.dhs.gov

002836

TABLETOP THE VOTE 2019
REGISTRATION FORM

CISA
CYBER+INFRASTRUCTURE

Tabletop the Vote 2019: National Election Cyber Virtual Tabletop Exercise

Please fill in all of the requested information on the registration form below for each participating video teleconference (VTC) location.

GENERAL INFORMATION

ORGANIZATION NAME:		
TYPE OF ORGANIZATION:	Choose an item	
STATE:		
REGION:		
PROJECTED NUMBER OF PARTICIPANTS:		
REQUESTED PARTICIPATION DATE: (Select dates and add location of exercise participants)	Primary date	Location
	Additional date	Location
HOW ARE YOU ATTENDING? (Select one)	In-person (Fed Gov't in NCR only)	

APPLICATION POINTS OF CONTACT

PRIMARY POC	NAME:		SECONDARY POC	NAME:
	EMAIL:			EMAIL:
	PHONE:			PHONE:

ON-SITE COORDINATION POINTS OF CONTACT

PRIMARY POC	NAME:		SECONDARY POC	NAME:
	EMAIL:			EMAIL:
	PHONE:			PHONE:

Note: Must be reachable during the VTTX.

INFORMATION TECHNOLOGY POINTS OF CONTACT

PRIMARY POC	NAME:		SECONDARY POC	NAME:
	EMAIL:			EMAIL:
	PHONE:			PHONE:
	PHONE NUMBER TO VTC LOCATION:			PHONE NUMBER TO VTC LOCATION:
	IP or ISDN#:			IP or ISDN#:

Note: Must be available to address technical issues during the VTTX.

All video teleconference (VTC) connections must be tested prior to the VTTX with the DHS Federal Emergency Management Agency (FEMA) Video Operations Center (VOC) by calling 1-540-542-2171 or emailing: fema-voc@fema.dhs.gov. Testing must be completed between May 15-31, 2019. Please inform the FEMA VOC that you are a participant in the National Elections Cyber Exercise and would like to request a test of your VTC capabilities. Once completed, please report the results of your test to CISA at CEP@hq.dhs.gov.

Continue to next page →

TABLETOP THE VOTE 2019
REGISTRATION FORM (cont.)

CISA
CYBER+INFRASTRUCTURE

Tabletop the Vote 2019: National Election Cyber Virtual Tabletop Exercise

GUIDANCE FOR REMOTE PARTICIPANTS

- Remote participation will allow state and county boards of election, in addition to other state/local equities, to participate from their home states as a cohesive group. States will need to consolidate their play from whatever primary location their state election office chooses if they want to participate via VTC.
- The number of individuals that you plan on inviting may help dictate what size room is best; however, states might have limited options available, since not all rooms are equipped with VTC capabilities. NCEPP suggests that states consider using their State Emergency Operations Centers, if available, since these locations are normally used for FEMA sponsored VTTX's and are equipped with VTC capabilities.
- Room setup: DHS recommends a U-shaped configuration for participants with the open side facing the front of the room/ screen to view the video teleconference and accompanying slides.
- Depending upon the size of the room, microphones may be needed to allow for effective communication between the room and the other participants on the VTC.

SUBMIT

TLP:WHITE

TRAFFIC LIGHT PROTOCOL (TLP)

FIRST Standards Definitions and Usage Guidance — Version 1.0

1. Introduction

a. The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST.

b. TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.

c. TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated sharing exchanges, but is not optimized for that use.

d. TLP is distinct from the Chatham House Rule (when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.), but may be used in conjunction if it is deemed appropriate by participants in an information exchange.

e. **The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance**.

f. **If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source**.

2. Usage

a. **How to use TLP in email**

TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.

b. **How to use TLP in documents**

TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12 point type or greater.

- **RGB:**
  TLP:RED : R=255, G=0, B=51, background: R=0, G=0, B=0
  TLP:AMBER : R=255, G=192, B=0, background: R=0, G=0, B=0
  TLP:GREEN : R=51, G=255, B=0, background: R=0, G=0, B=0
  TLP:WHITE : R=255, G=255, B=255, background: R=0, G=0, B=0
- **CMYK:**
  TLP:RED : C=0, M=100, Y=79, K=0, background: C=0, M=0, Y=0, K=100
  TLP:AMBER : C=0, M=25, Y=100, K=0, background: C=0, M=0, Y=0, K=100
  TLP:GREEN : C=79, M=0, Y=100, K=0, background: C=0, M=0, Y=0, K=100
  TLP:WHITE : C=0, M=0, Y=0, K=0, background: C=0, M=0, Y=0, K=100

TLP:RED

TLP:AMBER

TLP:GREEN

TLP:WHITE

3. TLP definitions

a. **TLP:RED** = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

b. **TLP:AMBER** = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

c. **TLP:GREEN** = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

d. **TLP:WHITE** = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Notes:
1. This document uses "should" and "must" as defined by RFC-2119.
2. Comments or suggestions on this document can be sent to tlp-sig@first.org.

From: Amy Cohen
To: Flynn, Julie; Kim Turner; Anthony Stevens
Subject: TTX Form
Date: Thursday, May 23, 2019 11:04:33 AM
Attachments: Tabletop the Vote 2019-Registration Form_v00[1].pdf

---

Hi all,

DHS let me know that they're still waiting on Virtual TTX forms from your state. If you are planning to participate, please complete and return the attached.

Thanks!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 4/5
Date: Friday, April 05, 2019 2:20:11 PM
Attachments: NASED Innovators Award_2019.pdf

Hello all!

Happy Friday – I can't believe we're in April already. Some news you can use below.

- As many of you are aware, the EAC Standards Board meets next week (April 10-12) in Memphis. On April 10 from 1-4pm, the EAC will host a public hearing on the VVSG 2.0 at which any interested party in attendance is welcome to provide comment. I would strongly encourage those of you who will be in town at that time to comment. This is a HAVA-mandated opportunity for the broader community to weigh in on both the content and the proposed structure of the VVSG 2.0; there is still the opportunity to submit a written comment by May 29, this is just an in-person opportunity. If you have any questions about the current situation or how we got here, please feel free to contact me and we can talk through it – I know it's confusing, but it's important to our entire field, especially as so many are contemplating voting equipment purchases.
- A reminder that the DHS national Virtual Table Top Exercise (VTTX) will take place **June 18, 19, 20**. For those of you who haven't done it before, the exercise is the same each day, but repeating it helps with scheduling. The event is virtual, but you'll want to get as many stakeholders as you can in one place so that you can simulate who you would get involved during an actual incident: local election officials, Homeland Security Advisors, National Guard, etc. You will be responsible for inviting your in-state players and for securing a facility in your state. You will need a large conference room to accommodate your group and video conference capability; last year, states used hotel ballrooms, state fusion centers, and local colleges or universities for space. Like an in-person TTX, the purpose is to simulate the time leading up to and on Election Day to talk through how you would handle each scenario; unlike an in-person TTX, you do not need to have space for people to run around and move from place to place. Please let me know if you have any questions. Last year, we had 44 states and DC participate, and I'm optimistic we will have similar levels of participation this year.
- Earlier this week at a joint meeting of the Executive Committees of the Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC), the SCC mentioned that the primary mechanism by which they get new members is when state and local election officials encourage their vendors to join. I've mentioned this before, but please encourage the election-related vendors in your state to join; this includes voting system vendors, but also voter registration system vendors, e-pollbook vendors, mail houses, print vendors, and more. To join, they can contact Chris Wlaschin (chris.wlaschin@essvote.com) and Bryan Finney (bryan@democracylive.com), who are the Chair and Vice Chair of the SCC, respectively. There's no financial cost to joining.
- The Center for Technology and Civic Life (CTCL) is doing a free webinar on voter registration

and automatic voter registration at Medicaid agencies on Thursday, April 11 at 1pm CT. Click here for more information and to register. Those of you who attended the February conference may remember that Whitney May presented during the non-profit session on the work that CTCL does.

- Last Friday and Saturday, the NASED Board held a productive meeting in DC to discuss some NASED business (like the award I sent out on Monday and have reattached!), start planning the summer conference, and meet with staff from several congressional committees. The entire day and a half was incredibly productive, and you will not be surprised to hear that your Board ably represented all of you in the meeting with Hill staff where we discussed nerd stuff ranging from the VVSG 2.0 to cybersecurity to street segments and GIS to help them understand how elections actually work.
- Last week, I sent out the link to book your room at the Omni for the summer conference in Austin, July 14-16. Several of you let me know right away that the link was broken, but it is fixed now, so book your rooms! Registration will open for all of you by the end of this month.

Have a lovely weekend, and if you care about March Madness, good luck and go sports!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 4/10
Date: Wednesday, April 10, 2019 2:43:52 PM
Attachments: Important HAVA Awards Update.msg
Draft FPCA and FWAB Available for Public Comment.msg

Hi all,

Looking forward to seeing many of you in Memphis this week!

- The EAC Standards Board is meeting in Memphis starting tomorrow, April 11-April 12. In conjunction with that, and consistent with the requirements in HAVA, the EAC is holding a public hearing on the VVSG 2.0 today, April 10, from 1-4pm CST, which you can watch via livestream here. The public comment period that I have been harping on, which is separate, is open until 4pm ET on May 29, 2019 and can be submitted to votingsystemguidelines@eac.gov. The 2.0 document is available on the EAC website, and here is the link. If you have questions or want to better understand what's going on, feel free to reach out.
- DHS is initiating the "Plus 3" phase of its election security clearance program, which will provide additional clearance opportunities for state and local government officials and private sector election infrastructure partners. Three additional election officials in each state will be nominated via the following process:
    - A state or local election official, nominated by the state chief election official;
    - The local representative to the EAC Standards Board (or their designee) in the state; and
    - A state or local election official, nominated by CISA regional staff (e.g. a Regional Director or Protective Security Advisor)

  There will also be opportunities for clearances for additional private sector partners though the Plus 3 program, but that does not impact the number of additional election official clearances. Please let me know if you have questions about the Plus 3 program or any other part of the clearance process.
- Many of you received the attached email from Mark Abbott at the EAC regarding the closing of round 1 of the HAVA grant. For questions, please contact Mark at mabbott@eac.gov.
- A reminder to cast your vote for the EI-ISAC executive committee! Link not included because only primary ISAC members are eligible to vote. **Voting ends Friday, April 12 at noon EST**. States only vote for state-level positions, but be sure to remind your local election officials to vote for their local representation.
- The Federal Post Card Application (FPCA) and the Federal Write-in Absentee Ballot (FWAB) are out for public comment again after the initial public comment period – see the attached email. Comments must be received no later than April 24, 2019.
- The EAC released a report on HAVA grant spending from FY 18. The report is available here.

Please let me know if you have any questions on the above, and if you're in Memphis, make sure to

say hello!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From:	Amy Cohen
To:	Amy Cohen
Subject:	Update, 4/12
Date:	Friday, April 12, 2019 5:23:07 PM
Attachments:	(FOUO) Survey on Foreign Influence Activities.pdf Message from the EI-ISAC - (UFOUO) Joint Intelligence Bulletin - New Information Reveals Russian Government Cyber Actors Likely Conducted Research and Reconnaissance Seeking Vulnerabilities in All US States" Election Infrastructure in 2016 - UFOUO.msg 4.10.19 Letter to State Elections Officials - Final[4][1].pdf

Good afternoon, all,

I know I've already sent multiple emails this week, but it's been a busy one. A few more things for your weekend reading list:

- On Wednesday, NASED and NASS received the attached letter from Zoe Lofgren, Chair of the US House Administration Committee, in which she asks for additional information on how each state and territory has spent their HAVA funds and asked that we share the letter with our members. Keith will respond from NASED, but NASED cannot comment on your individual states. NASS already distributed this to the Elections Committee and I sent this to the NASED Chief Election Officials.

  Chair Lofgren asks for responses by May 15, 2019, and you can send them to Tanya Sehgal, Majority Elections Counsel at Tanya.Sehgal@mail.house.gov.

- Earlier this week, Ars Technica published a story on the Joint Intelligence Bulletin that you received on March 27 about all 50 states being targets in 2016 and that was also sent by the ISAC (attached). This is not new information. Secretary Nielsen said it at our 2018 Summer Conference in Philadelphia, and others at DHS have said the same things in various other public settings, including during congressional testimony. This does not change the assessment that there were no votes changed in the 2016 election.

- The DHS Intelligence Cyber Mission Center (CYMC) tracks ongoing overt and covert influence activities, including a limited number of social media accounts suspected of being controlled by foreign influence actors, state controlled media and other state government affiliated websites. The CYMC is requesting feedback from partners to better understand the value and use of reporting on suspected state-sponsored influence operations targeting US audience. I&A is seeking to identify whether providing DHS stakeholders with insight into foreign influence activities—including trending topics and hashtags across social media platforms, state media, and suspected influence websites—would be valuable for those entities to carry out their missions and operations.

  The attached survey questions should only take a few minutes, and are intended to help assess the value of this reporting, the precise intended audience, and how it may be used by relevant stakeholders to accomplish mission-related tasks.

- Sen. Klobuchar's office shared a letter she sent to DHS and FBI urging them to form a joint task force to include social media platforms and state and local election officials to help identify and address misinformation/disinformation.

- At the Standards Board meeting yesterday, the EAC indicated that they had not contemplated policies around passing the VVSG, specifically whether the Requirements and Test Assertions are part of the VVSG or if it's just the Principals and Guidelines, or what would happen in the absence of a quorum. As a result, the VVSG subcommittee recommended, and the Standards Board unanimously passed, a recommendation that the VVSG is a standalone document required by HAVA and the Requirements and Test Assertions are established by policy. In addition, they recommended that any policy document have a provision for the Requirements and Test Assertions to be updated in the absence of a quorum.

  Note for all you West Coasters that there's likely to be another public hearing in association with the Board of Advisors in Salt Lake City on Tuesday, April 23 from 3-6pm.

Have a lovely weekend, all!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From:	Amy Cohen
To:	Amy Cohen
Subject:	Update, 4/19
Date:	Friday, April 19, 2019 3:31:02 PM
Attachments:	Tabletop the Vote 2018 National Election Cyber Tabletop Exercise AAR_v00 approved.pdf Standards Board Public Comment[2].docx MW Testimony US-EAC VVSG 04-10-2019[1].docx Request for Applications - NGA Policy Academy on Election Cybersecurity.pdf

Hi all,

Happy Friday!

- In case you've been completely off the grid for the last 24 hours or you've been watching the Beyoncé documentary on repeat, the Mueller report was released (volume 1 and volume 2). The pages related to election administration are pages 50-51 of volume 1.
- As you know, Kirstjen Nielsen is no longer the Secretary of Homeland Security; Kevin McAleenan is the Acting Secretary for DHS. Election security remains a priority for the agency and we can expect the same level of commitment that we had under Former Secretary Nielsen.
- Attached is an after-action report from last year's Virtual TTX. As a reminder, this year's Virtual TTX will be June 18, 19, and 20. An invitation will be coming soon, hopefully next week.
- Earlier today, Senator Klobuchar (D-MN) and 30 other senators sent a letter to the Senate Appropriations Subcommittee on Financial Services and General Government to increase funding to the EAC (funding was cut in the FY20 budget) and provide an additional $250 million in grants for state and local election offices. It does also sound like we could see something around a steady funding stream in the coming weeks/months, so stay tuned on that.
- Attached please find the testimony that Rob Rock (Rhode Island) and Meagan Wolfe (Wisconsin) delivered last week at the public hearing in Memphis prior to the EAC Standards Board meeting. Mark Goins (Tennessee) also testified; his main point "was that the process for developing and approving the VVSG is too slow. Within the confines of federal law, the new testing guidelines and assertions need to be implemented as soon as possible." There will be another public hearing on April 23 from 3-6pm MT, held in conjunction with the Board of Advisors meeting in Salt Lake City, UT. That hearing will be livestreamed on eac.gov.
- A reminder that the public comment period for the VVSG 2.0 ends on May 29 at 4pm ET. The NASED Board is working on a comment and will circulate it to all of you as soon as we can. The VVSG 2.0 document is available here.
- A reminder about the National Governor's Association application for its Policy Academy on Election Cybersecurity (attached). The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364). Applications are due by **8pm ET on May 10, 2019**. Both NASS and NASED worked with NGA

on the RFA itself and are helping to make sure this project is valuable for state election offices.

Have a lovely weekend!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 4/26
Date: Friday, April 26, 2019 2:29:26 PM
Attachments: Tabletop the Vote 2019-Registration Form_v00[2].pdf
Tabletop the Vote 2019_State Save the Date_v00[1].docx
4.10.19 Letter to State Elections Officials - Final.pdf
NASED Response to House Admin.pdf

Good afternoon, all!

- Attached please find an invitation to Tabletop the Vote 2019, the DHS Virtual TTX (VTTX), June 18, 19, and 20. Please follow the instructions to **RSVP by May 15, 2019**, and there is guidance on room size and set-up. Note that **you must test your video conference connection May 15-31** to ensure that everything is in working order. Instructions for how to test are also included in the pdf.
- As you remember, the Chair of the House Administration Committee sent NASED and NASS the attached letter earlier this month asking for additional details on your HAVA spending. You can respond to Tanya Sehgal (Tanya.Sehgal@mail.house.gov) by May 15, 2019 with additional information. NASED President Keith Ingram responded directly to Chairperson Lofgren, and the letter is also attached.
- Registration for our summer conference, July 14-16 in Austin, TX is now open! I will have a draft agenda for you early next week, but for your planning purposes, we'll start at 9am on Sunday, July 14 (breakfast at 8:30) and will conclude by 4:30pm on Tuesday, July 16. Tuesday will be for NASED members only and will be a mix of programming and open mic. I am working on planning (air conditioned) fun for Sunday night and Monday night.
    - Book your hotel room at the Omni Austin Downtown Hotel at the group rate of $145/night plus taxes. Please note that there is an error on the page and it says $146 when our rate is $145 (federal per diem). If you already booked, they will adjust the rate for you. Every dollar counts, right?
- As of today, NASED and NASS have spoken to Facebook, Twitter, and Google as part of our "stay in touch even when things are slower" initiative, and I want to update you on some changes in reporting misinformation. It is important to also keep me in the loop about what you're seeing and reporting so I can advocate for changes to the process as needed.
    - **Facebook**: if you see misinformation (statements of intent, calls for action, or advocating for violence due to voting, voter registration, or the outcome of an election; offers to buy or sell votes with cash or gifts; misrepresentation of dates, locations, times, or methods for voting or registering to vote; misrepresentation of who can vote, qualifications for voting, whether a vote will be counted, or ID), **email reports@content.facebook.com and copy Eva Guidarini (eguidarini@fb.com)**; if you don't copy Eva, we can't guarantee that your report will be reviewed. You must include as much information as possible, including a link or a screenshot of the bad post and a relevant link or copy of a statute or regulation, if available. If you believe your account has been compromised in some way, you should also email Eva.
    - **Google:** if you see misinformation on a Google platform (like Search or YouTube),

please email John Ruxton (johnruxton@google.com) and Erica Arbetter (arbetter@google.com). Examples of times to email them: when a partisan ad links to your site but doesn't include a "paid for" disclaimer, if a YouTube video includes inaccurate information about the mechanics of voting (ie – days and times are wrong), or if the information in the Discovery Box has the wrong Secretary of State. Google did not work with us in advance of the 2018 election, so this is a new process and I will be particularly interested in your feedback on how it works and how it can be improved.

    - **Twitter:** no changes here at this time (we're working on it). Please send me as much information as possible about the misinformation and I will report it. They define misinformation the same way that Facebook does.

- Congratulations to the members of the inaugural EI-ISAC Executive Committee
    - SOS: Barbara Cegavske (NV) and Nellie Gorbea (RI)
    - State Election Officials: Meagan Wolfe (WI) and Bob Giles (NJ)
    - State IT: Justin Burns (WA) and Trevor Timmons (CO)
    - Local Election Officials: Wesley Wilcox (Marion County, FL), Gary Sims (Wake County, NC), Tammy Smith (Wilson County, TN), Paul Adams (Lorain County, OH), and Jennifer Anderson (Hays County, TX)
    - Local IT: Joshua Helms (Greene County, MO) and Rahul Patel (Chicago and Cook County, IL)

Have a nice weekend!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/3
Date: Friday, May 03, 2019 11:22:33 AM
Attachments: Debunking_Handbook[2].pdf
Lewandowsky_PSPI_2012[1].pdf
NASED VVSG Comment_Final_5.2.19.pdf
Tabletop the Vote 2019-Registration Form_v00[2].pdf

Good morning all! A week so packed, you're hearing from me twice…

- Attached please find the comment that the NASED Executive Board submitted to the EAC as part of the VVSG public comment period. Feel free to borrow from it as needed for your own submissions. As a reminder**: comments must be received by 4pm ET on May 29, 2019** and can be submitted to votingsystemguidelines@eac.gov. Here is the link to the principles and guidelines; they are seeking comment on both the content of the principles and guidelines AND the structure (having the principles and guidelines, which are high level, be the VVSG 2.0, and the requirements and test assertions be separate).
- After soliciting feedback from all of the critical infrastructure sectors and subsectors, DHS released a list of National Critical Functions, and elections is on it. According to DHS, critical functions are "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." This list is significant because it demonstrates how DHS is viewing sectors as interdependent and is taking a risk-based approach, where the focus is less on the physical thing and more on the functions that thing does and the impact a disruption would have. You can learn more about the significance of the list here.
- The National Risk Management Center (NRMC) at DHS and the RAND Corporation are hosting an Election System Risk Assessment Experts' Group Workshop in Arlington, VA on **Wednesday, May 22**. The purpose of the workshop is to review and solicit feedback on analysis identifying potential cybersecurity vulnerabilities, their related consequences, and relative risk in election systems. They need volunteers for this effort and will be able to offer travel funding for state and local election officials who wish to participate. Participants from both state and local election offices, as well as from the vendor community, are welcome. Please RSVP as soon as possible to EISSA@hq.dhs.gov if you or someone in your office is interested.
- The DHS Countering Foreign Influence Task Force provided the attached academic paper and infographic on debunking misinformation because they thought you would find it valuable.
- A reminder to sign up for Tabletop the Vote 2019, the DHS Virtual TTX (VTTX), June 18, 19, and 20. Please follow the instructions in the attached to **RSVP by May 15, 2019**, and there is guidance on room size and set-up. Note that **you must test your video conference connection May 15-31** to ensure that everything is in working order. Instructions for how to test are also included in the attachment.

Have a great weekend!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/7
Date: Tuesday, May 07, 2019 12:58:28 PM
Attachments: NASED Innovators Award_2019.pdf
4.10.19 Letter to State Elections Officials - Final_From House Admin.pdf
Tabletop the Vote 2019-Registration Form_v00[2].pdf
RFA - Policy Academy on Election Security v3.docx
NASED Response to House Admin.pdf

Hi all,

Busy week so far! Lots of deadlines in the below.

- The U.S. House Administration Committee will hold a hearing tomorrow, May 8, at 2pm ET, on election security. The hearing will be livestreamed. Witnesses are:
    - Larry Norden (Brennan Center)
    - Marian Schneider (Verified Voting)
    - Joe Lorenzo Hall (Center for Democracy and Technology)
    - Michigan Secretary of State Jocelyn Benson
    - Alabama Secretary of State John Merrill
- The U.S Senate Rules Committee will hold a hearing on May 15th focused on EAC oversight. No additional information is available at this time, but I will send it around when I have it.
- Ryan Macias, Acting Director of Testing and Certification at the EAC announced that he is leaving the agency, effective Friday, May 17. After May 17, any questions should be directed to Jerome Lovato (jlovato@eac.gov). As you may recall, former Director of Testing and Certification Brian Hancock left the agency in March, and the job opening has been posted for several weeks. I will update you as I know more about the transition plans.
- Don't forget to apply for the NASED Innovators Award! Your applications are due to awards@nased.org by **this Friday, May 10 at 6pm PT**. The information about the award is attached.
- A reminder about the letter that House Admin Chair Zoe Lofgren sent to NASED and NASS, and that I've reattached for your reference. If you are planning to respond, responses are due to Tanya Sehgal, Counsel for the committee (Tanya.Sehgal@mail.house.gov) by **Wednesday, May 15.** The NASED response from President Keith Ingram is also attached again for your reference.
- A reminder to sign up for Tabletop the Vote 2019, the DHS Virtual TTX (VTTX), June 18, 19, and 20. Please follow the instructions in the attached to **RSVP by Wednesday, May 15**, and there is guidance on room size and set-up. Note that **you must test your video conference connection May 15-31** to ensure that everything is in working order. Instructions for how to test are also included in the attachment.
- Another, maybe final, reminder about the National Governor's Association application for its Policy Academy on Election Cybersecurity (attached). The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner

(mbrunner@nga.org; 202-624-5364). **Applications are due by 8pm ET on Friday, May 10.** Both NASS and NASED worked with NGA on the RFA itself and are helping to make sure this project is valuable for state election offices.

- Yesterday, Microsoft announced a new effort called ElectionGuard, an open-source software development kit (SDK), to help secure elections. They are working with several voting technology vendors to hopefully integrate this into voting machines.

Have a good weekend…just kidding, it's only Tuesday!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/10
Date: Friday, May 10, 2019 4:48:17 PM
Attachments: Tabletop the Vote 2019-Registration Form_v00[2].pdf
NASED Innovators Award_2019.pdf
Observer Qualifications and Application Process 2018.pdf

Happy Friday! A few more things to wrap up the week:

- Earlier this week I let you know that Ryan Macias will be leaving the EAC on May 17. Yesterday, the EAC announced that Jerome Lovato will be the new Director of Testing and Certification. Jerome has been at the EAC for two years working on voting system certification and risk-limiting audits. Prior to joining the EAC, he led voting system certification for the Colorado Secretary of State. Jerome can be reached at jlovato@eac.gov.
- Don't forget to submit your NASED Innovator Award submission by **6pm PT today**! Information attached and submissions are due to Awards@nased.org.
- A reminder to sign up for Tabletop the Vote 2019, the DHS Virtual TTX (VTTX), June 18, 19, and 20. Please follow the instructions in the attached to **RSVP by Wednesday, May 15**, and there is guidance on room size and set-up. Note that **you must test your video conference connection May 15-31** to ensure that everything is in working order. Instructions for how to test are also included in the attachment. If you have not yet submitted because you are still locking down a location, you can RSVP without it. You just need your location finalized to test.
- The Senate Rules EAC Oversight hearing on Wednesday, May 15th will be at 2:30pm ET. All four commissioners will be in attendance. The hearing will be livestreamed.
- Interested in observing international elections? Uncle Sam needs you! Attached is information on upcoming OSCE election observation missions in Kazakhstan on June 9 and Albania on June 30. Please contact Shannon Brink at the US State Department at BrinkSM@state.gov with questions.

Have a good weekend!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/15
Date: Wednesday, May 15, 2019 1:27:34 PM
Attachments: Tabletop the Vote 2019-Registration Form_v00[1][2].pdf
4.10.19 Letter to State Elections Officials - Final[1].pdf

Hi all,

So much going on.

- Today at 2:30pm ET, Senate Rules will hold an EAC oversight hearing. All four commissioners will attend. The hearing will be livestreamed.
- Representative Thompson (R-MS) and Representative Lofgren (D-CA) introduced the Election Security Act of 2019. I'm told most, if not all of this, pulls from the election security sections of HR 1.
- The House Government Oversight National Security Subcommittee will hold a hearing on May 22 at 2pm ET. Stay tuned for the final witness list, but I'm hearing that there will be representatives from the EAC, DHS, and at least one Secretary of State.
- Senator Lankford (R-OK), Senator Klobuchar (D-MN), Senator Peters (D-MI), and Senator Johnson (R-WI) introduced the Voting System Cybersecurity Act of 2019 today, which would add DHS to the TGDC.
- Senator Klobuchar (D-MN) and Senator Collins (R-ME) intend to introduce the Secure Elections Require Investment in Vigilant Staff Act (SERVIS Act) soon. This bill would establish a grant program administered by the EAC to cover up to 75 percent of the cost of the yearly tuition of election officials and employees who are enrolled in an accredited certificate program for election administration or cybersecurity. Eligible staff include state or local election officials, employees of a State or local election official, or an employee of the EAC. The bill would provide $1,000,000 for fiscal year 2021 and such sums necessary for each fiscal year between 2022 and 2028.
- According to the Washington Post, Senator Wyden (D-OR) will reintroduce the Protecting American Votes and Elections Act today, which will mandate paper ballots and post-election audits, as well as give DHS authority to set cyber security requirements for voting machines, databases, and results websites. It authorizes $500 M in grant funding for new voting equipment and $250 M for accessible ballot marking devices.
- On Monday, May 20 at 1:30pm ET, the EAC will hold the final public hearing on the VVSG 2.0. The hearing will be livestreamed. Witnesses will be:
    - Iowa Secretary of State Paul Pate
    - Traci Mapps, SLI Compliance
    - Jack Cobb, Pro V&V
    - Joseph Lorenzo Hall, Center for Democracy and Technology
- Speaking of the VVSG, the deadline for submitting public comment is fast approaching. **Comments must be received by 4pm ET on May 29, 2019** and can be submitted

to votingsystemguidelines@eac.gov. Here is the link to the principles and guidelines; they are seeking comment on both the content of the principles and guidelines AND the structure (having the principles and guidelines, which are high level, be the VVSG 2.0, and the requirements and test assertions be separate). The NASED Executive Board comment is available on our website for your reference.

- If you have not RSVP'd for the DHS Virtual TTX June 18, 19, and 20, the deadline to RSVP is today (also stop ignoring our emails, please ☺)! The RSVP form is attached. You can RSVP even if you don't know exactly where you will do the exercise from.
- Today is also the deadline to respond to House Administration Committee Chairperson Zoe Lofgren regarding her letter from April, which I've reattached for your reference.
- Wisconsin will hold a TTX "show and tell" event in Madison. It will be an actual TTX, with clerks from around the state, but we are also opening up the invitation to our state and federal election partners. There will be opportunities for election officials from other states to observe, moderate, and participate. Wisconsin has 1,853 local election jurisdictions, which can make training challenging. The Wisconsin Election Commission, however, has developed a model for conducting TTX's that they have used over 50 times in the last year+, and this is a valuable opportunity to learn how they have adapted the exercise to suit their state.

  When: Wednesday, June 5th from 9:00am-2:00pm
  Where: UW-Madison, Pyle Center, Madison, WI
  What: Election Security Table Top Exercise (TTX) using Wisconsin's train-the-trainer model. The Wisconsin Elections Commission, in partnership with Wisconsin's 1,922 municipal and county clerks, has conducted nearly 50 election security table top exercises in the last year and continues to expand the program as an ongoing training offering. The TTX event on June 5 is an opportunity for our state and federal partners to participate. The invitation to this event is being extended to Wisconsin partner agencies such as the Department of Military Affairs and the Division of Enterprise Technology along with Wisconsin legislators, election officials from other states and federal election partners. If you would like more information, please email Wisconsin Elections Commission Administrator Meagan.Wolfe@wi.gov and TTX Trainer Michelle.Hawley@wi.gov. If you will be attending, thye ask that you please complete this RSVP survey by **Monday, May 20**.
- Don't forget to register for the NASED Summer Conference in Austin, TX, July 14-16!

Please let me know if you have any questions!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/20
Date: Monday, May 20, 2019 12:52:00 PM
Attachments: AA_19-136_FSAgent[1].pdf

Happy Monday!

- Attached please find a document provided by DHS on some recent YARA rules, which are characteristics for identifying malware. While this will mostly not be meaningful to policy staff, please make sure your technical staff sees this and acts on it.
- Reminder that the EAC's last public hearing is this afternoon at 1:30pm ET. Livestream available here. Witnesses:
    - Iowa Secretary of State Paul Pate
    - Traci Mapps, SLI Compliance
    - Jack Cobb, Pro V&V
    - Joseph Lorenzo Hall, Center for Democracy and Technology
- The House Administration Committee will hold an EAC Oversight hearing tomorrow at 2:00pm that will be livestreamed. All four EAC commissioners will be in attendance. Testimony available here.
- The House Government Oversight National Security Subcommittee will hold a hearing on "Securing U.S. Election Infrastructure and Protecting Political Discourse" on Wednesday, May 22 at 2pm ET. I don't know if it will be livestreamed, but if it is, I will send it around when I have it. Witnesses will be:
    - Panel 1
        - Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS
        - Adam Hickey, Deputy Assistance Attorney General, National Security Division, US Department of Justice
        - Christy McCormick, Chair, EAC
        - Department of Defense (invited)
    - Panel 2
        - Bill Galvin, Massachusetts Secretary of State
        - Richard Salgado, Director of Law Enforcement and Information Security, Google
        - Nathanial Gleicher, Head of Cybersecurity Policy, Facebook
        - Kevin Kane, Public Policy Manager, Twitter

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660

Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 5/28
Date: Tuesday, May 28, 2019 4:49:07 PM
Attachments: notes-working-group-social-media-052119[2].pdf
Importance: High

Hi all,

I hope you enjoyed the long weekend!

- The EI-ISAC sent out an alert earlier this afternoon with the subject line "Message from EI-ISAC: DHS Information Sharing – Ukraine Elections-Related Threat Intel and IOCs – TLP: RED." **Please make sure you and your technical staff review this email promptly**. Because it is TLP: Red, I can't forward it to you.
- **Comments on VVSG v.2.0 are due tomorrow, Wednesday, May 29**. Late on Friday, the EAC announced a change to its VVSG comment process. **They are no longer accepting comments via email**. Comments can be submitted via form (9,000 character limit) or via mail to Voluntary Voting System Guidelines 2.0 Principles and Guidelines Comments, U.S. Election Assistance Commission, 1335 East-West Highway, Suite 4300, Silver Spring, Maryland 20910 – **comments submitted by mail must be postmarked by May 29**. There is a chance that the web form will be modified later today/tonight to allow for attachments, but I wouldn't count on that. Comments submitted previously via email still count. For your reference, the NASED Executive Board's comment is available here and here is a link to the Principles and Guidelines. They are accepting comment on both the content and the structure.
- DHS published this list of best practices for securing election infrastructure last week. This is based on issues that the Hunt and Incident Response Team (HIRT) has seen in their work on elections.
- Those of you participating in DHS's virtual TTX must **test your video hook up by this Friday, May 31**. Once you test, you must email CEP@hq.dhs.gov. TTX materials will be distributed on June 12 to give you time to print them and get everything ready. **This TTX is closed to the press** – you can do a press release or even a press conference afterwards saying that you participated, but the event itself is closed to the press. If you would like to have your vendors in the room, you are welcome to have them, but you need to invite them.
- The NASS/NASED Social Media Working Group held its initial call last Tuesday. Attached are the notes from that call. You will notice that each of the companies provided contact information for issues – don't feel shy about using it, but please also keep me in the loop so I have a good sense of what the issues are.
- Jennifer Morrell, risk-limiting audit expert, published a Practical Guide to Risk-Limiting Audits to provide a high-level overview of RLAs for state and local election officials; the companion Audit Implementation Workbook provides everything you need to know about how to conduct a ballot-comparison audit.

That's it for now.

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Amy Cohen
To: Amy Cohen
Subject: Update, 6/3
Date: Monday, June 03, 2019 1:51:21 PM
Attachments: Draft Member Agenda_06.01.19.pdf

Good morning all, and welcome to June!

- On Thursday of last week, the EAC extended the comment period on the VVSG 2.0 until **Friday, June 7**. Comments can be submitted via form (9,000 character limit), via upload on the EAC website, or via mail to: Voluntary Voting System Guidelines 2.0 Principles and Guidelines Comments, U.S. Election Assistance Commission, 1335 East-West Highway, Suite 4300, Silver Spring, Maryland 20910. Comments submitted previously via email still count. For your reference, the NASED Executive Board's comment is available here and here is a link to the Principles and Guidelines. They are accepting comment on both the content and the structure.
- Senator Lankford (R-OK) is expected to reintroduce the Secure Elections Act this week with some modifications to the bill introduced last year. According to press reports, the bill will strengthen information sharing between the federal government and state and local election officials, as well as require post-election audits; there will not be funding attached to the bill, but it will require all jurisdictions to implement audits if they want future funding.
- The House Financial Services and General Government Subcommittee will markup this FY2020 appropriations bill today at 7pm ET (happy Monday, indeed!). The bill provides funding for the EAC and additional grant funding for states provided through the EAC. States would be required to use the funds to replace DRE voting equipment (including, I think, DRE with VVPAT) with paper ballots or ballot marking devices and would be required to allocate at least 50% of the funds given to each state to local jurisdictions responsible for the administration of elections. States that have already replaced their voting equipment with machines that meet the requirements in the bill would be permitted to use the funds on "other authorized activities to improve the administration of elections…". There is a 5% state match required in the bill, too.
- Attached is a draft member agenda for the upcoming NASED Conference in Austin, July 14-16; still filling some things in, including fun, but it's coming together. Don't forget to register if you haven't done so already. Prices go up June 21!
- Upcoming events:
    - NCSL is getting ready for redistricting and has five seminars "coming up" (in quotes because some of them are in 2020 or 2021, not because they're not real):
        - June 20-23, 2019 | Providence, R,I. | Providence Marriott Downtown (here's the agenda)
        - Oct. 24-27, 2019 | Columbus, Ohio | Sheraton Columbus Hotel at Capitol Square
        - May 6-10, 2020 | Las Vegas | Renaissance Las Vegas Hotel
        - Sept. 24-27, 2020 | Portland, Ore. | Portland Marriott Downtown Waterfront
        - January 2021 | Washington, D.C. | Hotel and exact date TBD

That's all for now!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

From: Bhanu Pothugunta
To: Colleen McCormack
Subject: Webex meeting invitation: NH 2FA Demo
Date: Wednesday, October 10, 2018 10:04:42 AM

Hello,

Bhanu Pothugunta invites you to join this Webex meeting.

NH 2FA Demo
Wednesday, October 10, 2018
1:00 pm | Eastern Daylight Time (New York, GMT-04:00) | 1 hr
Meeting number (access code): 798 564 390
Meeting password: Vr4GXcqc

Add to Calendar

When it's time, join the meeting.

Join by phone
+1-650-429-3300 Call-in number (US/Canada)
Global call-in numbers

Can't join the meeting?

IMPORTANT NOTICE: Please note that this WebEx service allows audio and other information sent during the session to be recorded, which may be discoverable in a legal matter. By joining this session, you automatically consent to such recordings. If you do not consent to being recorded, discuss your concerns with the host or do not join the session.

Working Group Descriptions

(Joint) SSP WG: Update the Election Infrastructure Subsector-Specific Plan to reflect both GCC and SCC goals, objectives, and strategic path forward to effect those initiatives.
(Joint) EI NIST Cybersecurity Framework Profile WG: Apply the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity to the EIS to assist administrators and vendors in managing cyber-related risk in election systems. Implement NIST Framework standards, guidelines, and practices, including public-private coordination through the Critical Infrastructure Cyber Community Voluntary Program. Pursuant to the Roadmap to Secure Voice and Data Systems, determine the standards recommended by such bodies as NIST in regards to organizational responsibilities for implementing cybersecurity policies and procedures.
(Joint) Digital Network Development WG: Create and utilize a digital network that links all State and local election officials with each other and with GCC approved support organizations, services and products. Design and adopt a Digital Communication Portal (DCP) capable of reaching all election officials to enhance communications and support efforts from the Federal level down, from the State level down, and from the local level up.
(Joint) Disaster Recovery/Continuity Planning WG: Disaster recovery/continuity planning for natural disasters that affect multiple states or regions, or other pervasive non-cyber threats, geared toward developing Incident Response Plans.
(GCC) Communications WG: Ensure timely information sharing and consumption throughout the sector to promote clear communication about security threats, probabilities, vulnerabilities, controls and responses. Establish information sharing procedures and protocols, which will serve as the focal point of communication and coordination between Federal and SLTT election officials on matters specific to the security and integrity of elections. Implement an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant Subsector information, intelligence, and incident reporting.
(GCC) Strategic Communications/Public Affairs WG: Employ a strategic communications effort to ensure that the election profession is able to define, shape or otherwise participate in the public narrative around elections security in America. Develop and refine an outward facing strategic communications plan
(GCC) Capacity Building WG: Support efforts that will increase election officials' capacity to defend against, detect and recover from security incidents and ensure a common understanding and approach to building resilience. Continually review and modify as needed the Subsector's objectives, risk environments, priorities, mitigations, and available resources. Educate State and local election officials regarding cybersecurity services and resources available from DHS, EAC, MS-ISAC, and other public and private institutions.
(GCC) Resourcing & Funding Support WG: Work to establish consistent sources of funding that are appropriately flexible, to support the Subsector's cyber resilience and national security efforts. Work as a Council to identify election infrastructure security and resource gaps, collaborate with partners to identify funding needed to fill those gaps, and provide a forum to discuss election policy and resources needs to improve homeland security capabilities, such as trainings, Webinars, or toolkits.
(T)Training & Exercise WG: Collaborate on exercise opportunities and development of Training and TTX options for state and locals.

Joint GCC-SCC Working Groups

WG Name	Chair/CoChair(s)	GCC Reps	SCC Reps	Partners/SMEs	SSA Support	NOTEs:
SSP	Judd Choate, GCC Kay Stimson, SCC	TBD	TBD	Noah Praetz Leslie Reynolds Amy Cohen, NASED	Juan Figueroa Jimmy Tipton	Chair meetings in progress to develop drafting plan.
NIST Cybersecurity Framework	John Messina, NIST Laura Carlson, CISA Rahul Patel, Cook County (IL) Chris Wlaschin, SCC		Traci Mapps Jesse Peterson Matt Horace Nicole Nolette Vishal Hanjan Jessica Bowers Ed Smith	Gary Coverdale, SLTTGCC Eric Gookin, IA Amy Cohen, NASED	Jim Smith Jimmy Tipton	Initial WG scheduled for 3/14/19.
Digital Network Development	Neal Kelley, GCC Ericka Haas, SCC Brian Newby, EAC	Jamie Shew Tom Hicks Amber McReynolds Lori Augino Sarah B. Johnson Chris Chambless	Traci Mapps Jesse Peterson Monica Childers Afua Twumasi-Ankrah Kay Stimson Matt Horace Donetta Davidson	Tamsin Harrington, DHS Ben Spear, EI-ISAC Amy Cohen, NASED	Amy Rue	Ongoing discussions between WG chairs to develop progress plan.
Disaster Recovery/Continuity Planning	Brian Newby, EAC	Christy McCormick	TBD	Gary Coverdale, SLTTGCC Mike Senyko, MI Eric Gookin, IA Amy Cohen, NASED	Jim Smith	TBD

GCC Working Groups

WG Name	Chair/CoChair(s):	GCC Reps	Partners/SMEs:	SSA Support Lead	NOTEs:
Communications	Ricky Hatch	Hon. Connie Lawson Hon. Maggie T. Oliver Hon. Jim Condos Neal Kelley Linda Lamone David Stafford Bob Zehentbauer Amber McReynolds Michael Winn	Brandon Clifton Leslie Reynolds Amy Cohen, NASED Marci Andino Megan Wolfe, WI	Jimmy Tipton	Published EI Communication Protocols in July 2018.
Strategic Communications/ Public Affairs	TBD: CISA/ESI ExCom P.A. Rep	Hon. Maggie T. Oliver Brad King Sarah B. Johnson Jake Spano Christy McCormick	Brenda Soder, EAC Amy Cohen, NASED Maria Benson, NASS Tim Mattice, EC Cindy Taylor, DHS Scott McConnell, DHS Herb Josey, DHS Jeanie Moore, DHS Kai Schon, WY Reid Magney, WI Kathryn Boockvar, PA Mike Senyko, MI	n/a	Formally adopted at 7/13/18 GCC meeting. WG Chairs TBD.
Capacity Building	TBD	Hon. Maggie T. Oliver Christy McCormick Chris Chambless Scott Konopasek Keith Ingram Jamie Shew	Nikki Charlson (MD) Amy Cohen, NASED	TBD	Formally adopted at 7/13/18 GCC meeting. Need to ID chair and begin meeting.
Resourcing & Funding	TBD	Hon. Jim Condos Linda Von Nessi	Amy Cohen, NASED	TBD	
(T) Training & Exercise	Bob Giles	TBD	Noah Praetz Amy Cohen, NASED		Discussed at ExCom level but not formally adopted; ExCom concurrence required.

Colleen McCormack

From: Hawley, Michelle R - ELECTIONS <Michelle.Hawley@wisconsin.gov>
Sent: Tuesday, May 28, 2019 3:09 PM
To: Colleen McCormack
Cc: Wolfe, Meagan - ELECTIONS
Subject: RE: State of Wisconsin Election Security Tabletop Training Exercise
Attachments: Moderator tips 20190222.pdf

Hi Colleen:

Thank you so much! For your reference, I've attached a tip sheet that we provide to help guide our moderators. One of our staff members will also go through the exercise materials with you that morning.

We will have access to the room starting the morning of the event. I expect that our staff will arrive around 7:30 a.m. to start setting up, should you care to join us (you are more than welcome - do not feel obligated). It doesn't take us too long to put things together.

We look forward to seeing you next week! Should you have any other questions or concerns, please do not hesitate to contact me or Meagan.

Sincerely,

Michelle R. Hawley
WisVote Training Officer
Wisconsin Elections Commission
608-261-2004
Michelle.Hawley@wi.gov

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, May 28, 2019 1:41 PM
To: Hawley, Michelle R - ELECTIONS <Michelle.Hawley@wisconsin.gov>
Subject: RE: State of Wisconsin Election Security Tabletop Training Exercise

Michelle,
I would love to participate in the exercise.
I will actually arrive early afternoon on June 4th in Madison.
If you need help with set up or anything, just let me know.
My mobile number is: [redacted]
See you soon.

Thank You,

Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Hawley, Michelle R - ELECTIONS [mailto:Michelle.Hawley@wisconsin.gov]
Sent: Tuesday, May 28, 2019 2:15 PM
To: Colleen McCormack
Subject: State of Wisconsin Election Security Tabletop Training Exercise

Hi Colleen:

I am working to fill roles for next week's TTX. We are expecting a few election administrators from other states, and Meagan mentioned that perhaps you might like to be more than an observer for the exercise. I'm writing to inquire whether you are interested in being a moderator (no worries, we will provide you with instructions that morning).

Please let me know whether you are interested in participating as a moderator in this exercise. We look forward to seeing you next week. Thank you!

Sincerely,

Michelle R. Hawley
WisVote Training Officer
Wisconsin Elections Commission
608-261-2004
Michelle.Hawley@wi.gov

Moderator Tips

This is a collection of tips, in no particular order, based on the experience of WEC moderators conducting the tabletop exercise for various groups around the state.

- Feel free to make up answers to small-scale questions about the scenario, such as the number of polling places in a municipality. Having a consistent answer throughout a simulation is more important than being "correct."
- Encourage participants to get up and talk to the participants at the other tables. If a participant says, "I would talk to the state," for example, encourage the participant to get up and walk over to the state table. This promotes keeping other participants at other tables involved in your decision making, as well as providing context clues to your own simulation.
- Try to get everyone involved. If a participant at a table is taking a back seat, start directing injects specifically to that person if it doesn't necessarily make sense. In the real world, it is not uncommon for emails and phone calls to end up where they do not belong.
- Fill in for the media. If there are no media moderators, or if the media moderators are busy elsewhere, you can fill that role by telling participants that a reporter is asking questions about an inject.
- Make sure everyone is having fun. Participants learn more and remember better when they are engaged. Make small-talk in between injections. Allow participants to make light of situations, so long as they also respond to them. Interrupt dull moments with flavor injects.
- Some participants may be reluctant to engage. If they are not responding to injects, put the pressure on them by saying that reporters are calling, or voters are threatening to sue.
- Allow for conversation. If there is debate about how to address an issue, let the participants come to their own solution even if you may disagree. This is their simulation, and any outstanding questions can be addressed in the TTX debrief.
- Feel free to talk to other moderators or the director of the TTX if you have any questions.
- Review the "flavor injects" before the start of the TTX and determine when you might want to incorporate them. While the "flavor injects" can be used in the TTX at any time, some might cause more debate than others, and it is good to be aware of the overall timeframe of your table.
- Flavor injects for counties and the state can, at the moderator's discretion, reference either a municipality that is being represented, or one that is not. In general, it is easier to reference an inject to a municipality that is not represented in the TTX than to try to coordinate flavor injects. In these cases, the discussion of that inject should take place amongst participants only at that table and the result of that discussion does not need to be communicated to participants at other tables. If a county moderator says an event happened at a municipality, but that municipality moderator has not drawn that inject, it causes confusion.

Colleen McCormack

From: Hawley, Michelle R - ELECTIONS <Michelle.Hawley@wisconsin.gov>
Sent: Wednesday, May 22, 2019 4:54 PM
Subject: Details for State of Wisconsin Election Security Tabletop Training Exercise (TTX)
Attachments: Guidance for June_5_2019 TTX.pdf

Dear Attendees:

Thank you for your interest in participating in and/or observing the State of Wisconsin Election Tabletop Training Exercise (TTX) created for our local election officials. This email contains an attachment with additional information about the exercise. Please note that we made a minor adjustment to the time of the event to allow for the exercise and an after action report.

Should you have any additional questions or concerns, please do not hesitate to email Meagan.Wolfe@wi.gov and Michelle.Hawley@wi.gov. Thank you and we look forward to seeing you on June 5th!

Sincerely,

Michelle R. Hawley
WisVote Training Officer
Wisconsin Elections Commission
608-261-2004
Michelle.Hawley@wi.gov

Colleen McCormack

From: Hawley, Michelle R - ELECTIONS <Michelle.Hawley@wisconsin.gov>
Sent: Tuesday, June 04, 2019 11:45 AM
Cc: Wolfe, Meagan - ELECTIONS
Subject: Final Confirmation and Details for State of Wisconsin Election Security Tabletop Training Exercise (TTX) - (Wednesday, June 5, 2019, 8:30am-12:30pm)
Attachments: Guidance for June_5_2019 TTX.pdf; TTX Agenda 20190605.pdf

Dear Attendees:

Please let this email serve as the final confirmation for tomorrow's State of Wisconsin Election Security Tabletop Training Exercise (TTX). Attached please find a revised data sheet (the **address for the parking structure is 415 Lake Street, Madison** – please forgive the typo in the original document), in addition to a copy of the agenda.

Again, thank you for your interest in participating in tomorrow's event. Should you have any questions, or are no longer able to attend, please be sure to contact Meagan.Wolfe@wi.gov and Michelle.Hawley@wi.gov. We look forward to seeing you tomorrow!

Sincerely,

Michelle R. Hawley
WisVote Training Officer
Wisconsin Elections Commission
608-261-2004
Michelle.Hawley@wi.gov

Wisconsin Elections Commission
Elections Security
Tabletop Training Exercise (TTX)

AGENDA

Date: Wednesday, June 5, 2019

Time: 8:30 a.m. to 12:30 p.m.

Location: Pyle Center
720 Langdon Street, Room 213
Madison, Wisconsin 53706

8:30 a.m. – 8:50 a.m.	Introductions / What is a Tabletop Exercise?
8:50 a.m. – 9:20 a.m.	Phase I – Planning / Existing Security Measures Discussion
9:20 a.m. – 9:30 a.m.	Break
9:30 a.m. – 10:55 a.m.	Phase II – Scenario Overview / Election Day Tabletop Exercise (TTX)
10:55 a.m. – 11:25 a.m.	What are the "right" answers for exercise? / After Action Review (participant level)
11:25 a.m. – 11:40 a.m.	Break
11:40 a.m. – 12:30 p.m.	Lessons Learned – Debrief for Observers (all are welcome)

Wisconsin Elections Commission

212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

Election Security Tabletop Training Exercise (TTX)

Thank you for your interest in participating in and/or observing the State of Wisconsin Election Security Tabletop Training Exercise (TTX) created for our local election officials. This is to provide you with additional information about this exercise.

WHEN: Wednesday, June 5, 2019

TIME: 8:30 a.m. to 12:30 p.m.

WHERE: Pyle Center
702 Langdon Street, Room 213
Madison, WI 53706

PARKING: The State Street Campus Parking Garage is located at 720 Lake Street, Madison and within walking distance of the Pyle Center (see page 2 for map).

PARTICIPANTS: Wisconsin Election Officials (county and municipal clerks) have been invited to participate in an Election Security Tabletop Training Exercise (TTX) to assess the effectiveness of their existing knowledge, policies, and practices as they relate to election security, to increase their awareness and preparedness, and to provide them with tools to ensure elections in the State of Wisconsin remain secure.

OBSERVERS: Since rolling out our TTX in May 2018, the Wisconsin Elections Commission has received numerous requests from local, state, and federal election security partners to observe and/or participate in our exercise. We are excited to extend this invitation and share our experience.

As indicated above, we invited local municipal clerks to participate in this training, most of whom have never experienced the exercise. Generally, this training is not observed by anyone outside of the participants and WEC staff/regional trainers. We aim to provide a training environment where elections officials can feel safe to make decisions and perhaps mistakes, without judgment and free of potential real-life ramifications. We recognize that inviting observers could potentially sway the willingness of participants to contribute. We respectfully request that the observers keep this in mind while observing to help foster an environment of learning for all our election partners.

MEALS: A light breakfast and refreshments will be provided on the morning of June 5. There are many dinner and lunch dining options within walking distance.

HOTELS: For overnight lodging, there are hotels relatively close to the Pyle Center:

Lowell Center
610 Langdon Street
Madison, Wisconsin
Phone: 608-256-2621

Graduate Madison
601 Langdon Street
Madison, Wisconsin
Phone: 608-257-4391

Hampton Inn & Suites
440 W. Johnson Street
Madison, Wisconsin
Phone: 608-255-0360

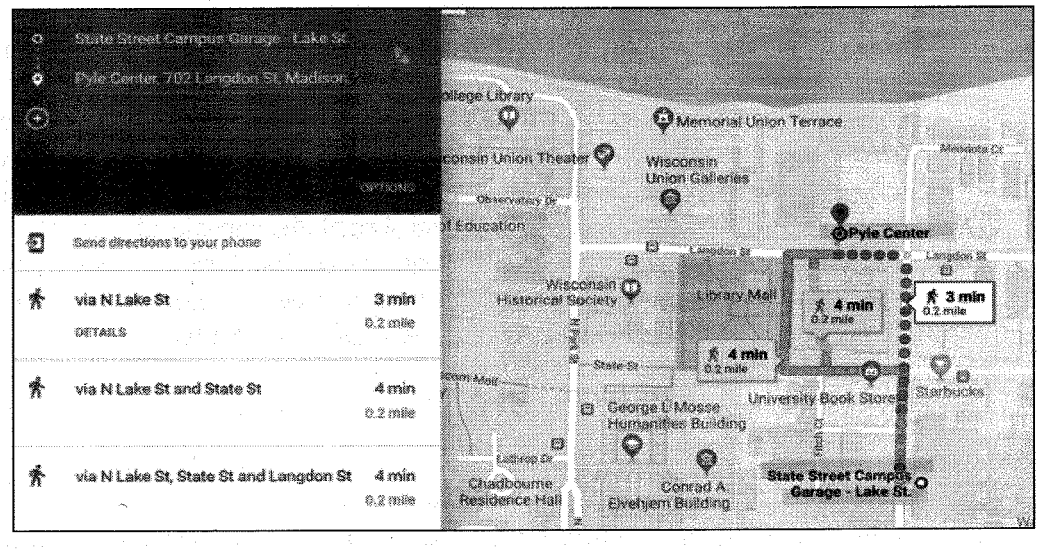
DoubleTree by Hilton
525 W. Johnson Street
Madison, Wisconsin
Phone: 608-251-5511

AIRPORT: Dane County Regional Airport (airport code MSN)
4000 International Lane
Madison, Wisconsin 53704

There is no public transportation that will easily take you to your hotel. WEC staff recommends using a taxi cab or a ride share service. Alternatively, the Milwaukee Airport (MKE) is about a one-hour drive from the event and the Chicago-O'Hare Airport (ORD) is about a two-hour drive from the event.

Should you have any other questions or concerns, or require any special accommodations, please do not hesitate to email Meagan.Wolfe@wi.gov and Michelle.Hawley@wi.gov. We look forward to seeing you on June 5!

State Street Campus Garage: 720 Lake Street, Madison, WI 53706
Pyle Center: 702 Langdon Street, Madison WI 53706



Colleen McCormack

From: Wolfe, Meagan - ELECTIONS <Meagan.Wolfe@wisconsin.gov>
Sent: Tuesday, June 04, 2019 12:20 PM
To: 'piercec1@michigan.gov'; 'anussmeyer@iec.in.gov'; Colleen McCormack; 'justinlee@utah.gov'
Cc: Hawley, Michelle R - ELECTIONS
Subject: Traveling to Madison

Election Colleagues-

We are excited that you will be joining us for tomorrow's TTX event in Madison, WI!

I apologize for getting this out later than I had intended, but I wanted to invite you to stop by the Wisconsin Elections Commission office today or tomorrow, should your schedule allow!

If there are any other projects or initiatives that you are working on or are interested in, I'm sure our team would be thrilled to discuss while you are in town!

Our office is located at 212 East Washington Avenue, Madison, WI We are right off the Capitol Square. When you get to our building, take the elevator to the third floor. Speaking of the Capitol, if you have time, you should check it out! It's the nation's most open Capitol and you can walk in and throughout the building at anytime between 8am and 6pm (later if the legislature is in session, which they are this week. Hearings and sessions are also open to the public to observe)

Also, if you need anything at all while you are in town, please feel free to call, text, or email me, anytime. My cell phone number is [redacted]

We expect tomorrow's TTX to end around 12:30. After, I was going to see if anyone was interested in lunch at the UW Union Terrace, nearby. It's a beautiful spot right on Lake Mendota https://union.wisc.edu/visit/terrace-at-the-memorial-union/ . If your schedule allows and if the weather cooperates, we'd be glad if you could join!

Welcome to Madison, and please let me know if there is anything we can do while you're here!

Meagan

Meagan Wolfe
Administrator
Wisconsin Elections Commission

Desk: (608) 266-8175
Cell: [redacted]
meagan.wolfe@wi.gov

Tabletop Exercise (TTX)
Response Tracker

Role in TTX: Fremont County

Time	Inject (Brief Description)	What action(s) would you take?
6 AM	Thunderstorm watch	Not much to do, watch weather
6:32	thunderstorm warning	Wyndham- check on Roads
7:50	Flashflood warning	touch base with Emergency Mgmt
8:00	signed wrong line in poll Book	document
8:30	flooding	Wyndham has flooding - prepare to move if needed
8:47	Power outage	- prepare paper ballots
9:20	flooding	~~Wyndham moving to Blue Gap~~ Blue Gap moving to School in Windham Call Sheriff to assist; Media release
10 AM	electioneering	
	missing voters in Redvale	- No calls yet on missing voters
10:27 AM	Press release	Vote open - issues at Windham

Time	Inject (Brief Description)	What action(s) would you take?
10:40	supplemental list	- State sending list of deactivated voters ERIC 2
10:50	buying votes	bake sale
11:39	Evacuation	Windham moving - bowling Alley
12:05	Media	not allowed to interview voters in line move to exit
1:07pm	moving polling place Windham + Blue Gap Send media release 1:45 - 2:45pm	
1:30pm	election programming - program our own breached	
1:57	polling place Send press release	open til 9pm Windham + Blue gap
3:25	Blue Gap	confirm someone is ready from State
5:23	MyVote	- directing voters to vote at Disney
5:45	Windham	ballot count off by 80

Tabletop Exercise (TTX)
Response Tracker

Role in TTX: _____

Time	Inject (Brief Description)	What action(s) would you take?
	AG check	EPM - + RSA's books on hand
	ERP	No mandate - pro active but highly recomend -
		7-8 regions - City clerks + the trainers Do Not get paid Volunteer
		3 people @ every table challenging Media inputs — level of improve - camera + interviews - press statements
		PIO - public info officer cyber - bring it down !! ?? Emergency mg't Nat'l Guard * Road Agents
		* Sheriff's office - state troopers * motivations -

Fremont County Script

6:00 AM – **Flood 1** plays automatically

6:30 AM – **Flood 2** plays automatically

7:45 AM – **Flood 3** plays automatically

8:30 AM – **Fake 3** appears on screen

11:00 AM – Hand out **Flood 6**

11:30 AM – MidVote 6 appears on screen

1:15 PM – Read **Programming 1** aloud to participants **(Media Inquiry)**

1:30 PM – Programming 2 appears on screen

3:00 PM – Hand out **Email 1 (Note to moderator: Email 1 contains malicious link. If participant chose to click link, run Email 3 scenario at 4:15 PM)**

3:30 PM – Read **Programming 4** aloud to participants

4:15 PM – Read **Email 3** aloud to participants **(Note to moderator: SKIPPABLE based on actions taken during Email 1 at 3:00 PM)**

4:45 PM – Hand out **Programming 5**

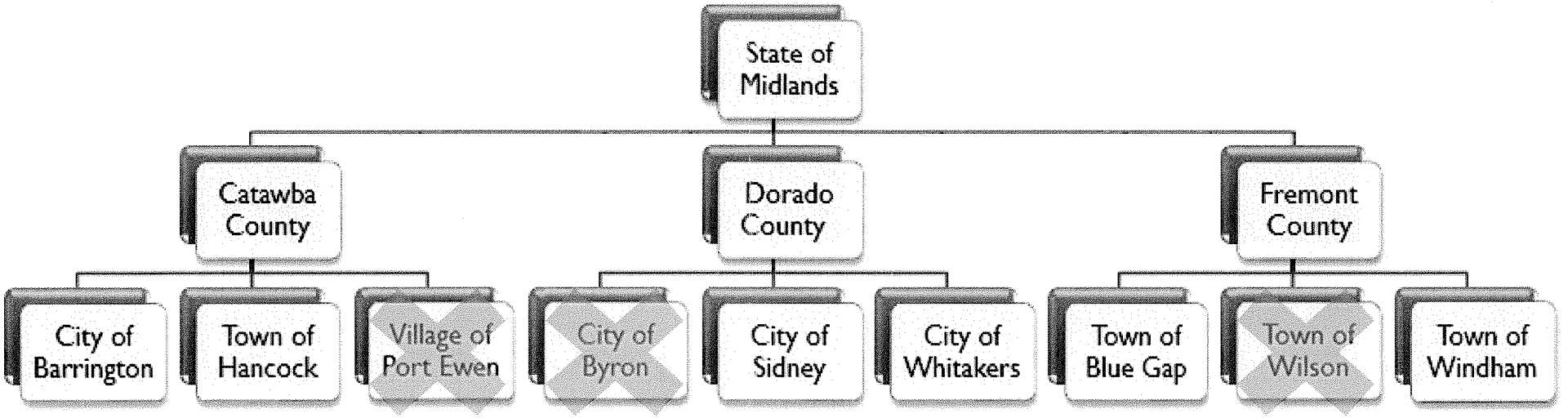
5:30 PM – **Car 4** appears on screen

6:30 PM – **Car 5** appears on screen

7:00 PM – Hand out **DDOS 1**

002883

THE STATE OF MIDLANDS



Fremont County

Fremont County

Wisconsin Elections Commission
Elections Security
Tabletop Training Exercise (TTX)

AGENDA

Date: Wednesday, June 5, 2019

Time: 8:30 a.m. to 12:30 p.m.

Location: Pyle Center
720 Langdon Street, Room 213
Madison, Wisconsin 53706

8:30 a.m. – 8:50 a.m.	Introductions / What is a Tabletop Exercise?
8:50 a.m. – 9:20 a.m.	Phase I – Planning / Existing Security Measures Discussion
9:20 a.m. – 9:30 a.m.	Break
9:30 a.m. – 10:55 a.m.	Phase II – Scenario Overview / Election Day Tabletop Exercise (TTX)
10:55 a.m. – 11:25 a.m.	What are the "right" answers for exercise? / After Action Review (participant level)
11:25 a.m. – 11:40 a.m.	Break
11:40 a.m. – 12:30 p.m.	Lessons Learned – Debrief for Observers (all are welcome)

Breaking News: Elections hacked!

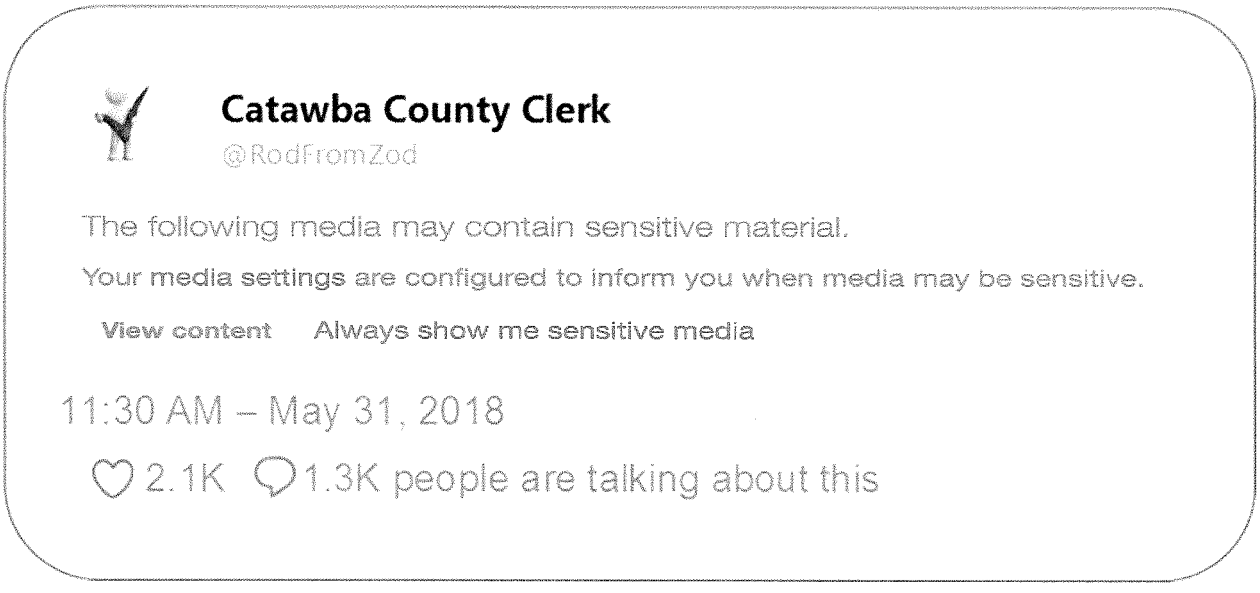
By DYLAN SMITH NOVEMBER 6, 2018

The Midlands Elections Commission has reported that it suffered a significant breach two months prior to the election, which enabled an attacker to remove over 5,000 voters in major metropolitan areas throughout the state. At this time, it appears that the attacker was specifically targeting foreign-looking voter names, perhaps attempting to sway the election in favor of the Liberty Party. The Elections Commission confirmed that the breach has been closed, and that in the future similar attacks will be blocked by the new multi-factor authentication system for its voter registration database.

Did Catawba County Clerk tweet bigoted remarks?

By DYLAN SMITH NOVEMBER 6, 2018

Early Election Day morning, residents of Catawba County were shocked to see a tweet from a Twitter user calling themselves the Catawba County Clerk who appeared to be making disparaging remarks regarding immigrant voters. At press time, this reporter was unable to confirm whether or not the account actually has any connection to the Catawba County Clerk's office, but Twitter sleuths are already beginning to make connections between this tweet and the difficulties being faced this morning by voters at the polls.



EVACUATION WARNING

You are **WARNED** that current or projected hazards associated with an emergency in this area **may** require immediate evacuation.

- This is the time for final preparation, precautionary movement of persons with special needs, mobile property, and perhaps even pets and livestock.
- Authorities will make every attempt to advise the public as conditions change. Area media outlets have been asked to broadcast updates as they are given.
- If you are not enrolled in **SMART 911**, now is the perfect time to do so. Log on to ***smart911.com*** and create your safety profile. This service will enhance your ability to receive alerts and provide information to responders to enhance your family's safety.
- DO NOT WAIT for authorities to give an evacuation order for your area. Early self-evacuation ensures the safety of you and your family.
- Please do not remove any exterior flagging or markings that have been placed outside of your home. These markings help emergency responders to identify who has or hasn't received notification.

If the emergency event escalates, emergency personnel may not have time to make personal notifications. If a slow moving emergency vehicle with lights and alternating siren tones is moving through the area, it is time to evacuate!

Evacuation Warning
Issued on:
Issued By:

[As audio flood warning]

THE NATIONAL WEATHER SERVICE IN SULLIVAN HAS ISSUED A THUNDERSTORM WARNING FOR THE COUNTIES OF FREMONT, JAMESON, AND HARRISON COUNTIES... UNTIL 6:15 PM TUESDAY

At 5:24 PM Doppler radar indicated a severe thunderstorm capable of producing heavy winds and moving West at 35 mph.

Severe thunderstorms produce damaging wind, deadly lightning and very heavy rain. For your protection move to an interior room the lowest floor of your home or business. Heavy rains flood roads quickly so do not drive into areas where water covers the road. Continuous ground to cloud lightning is occurring with this storm. Move indoors immediately. Lightning is one of nature's leading killers. Remember if you can hear thunder you are close enough to be struck by lightning.

[As audio flood warning]

THE NATIONAL WEATHER SERVICE IN SULLIVAN HAS ISSUED A
FLASH FLOOD WARNING FOR THE COUNTIES OF FREMONT, JAMESON, AND HARRISON
COUNTIES... UNTIL 8:00 PM TUESDAY

UP TO 3 INCHES OF RAIN HAVE ALREADY FALLEN AND ADDITIONAL HEAVY RAIN is
likely THIS MORNING...

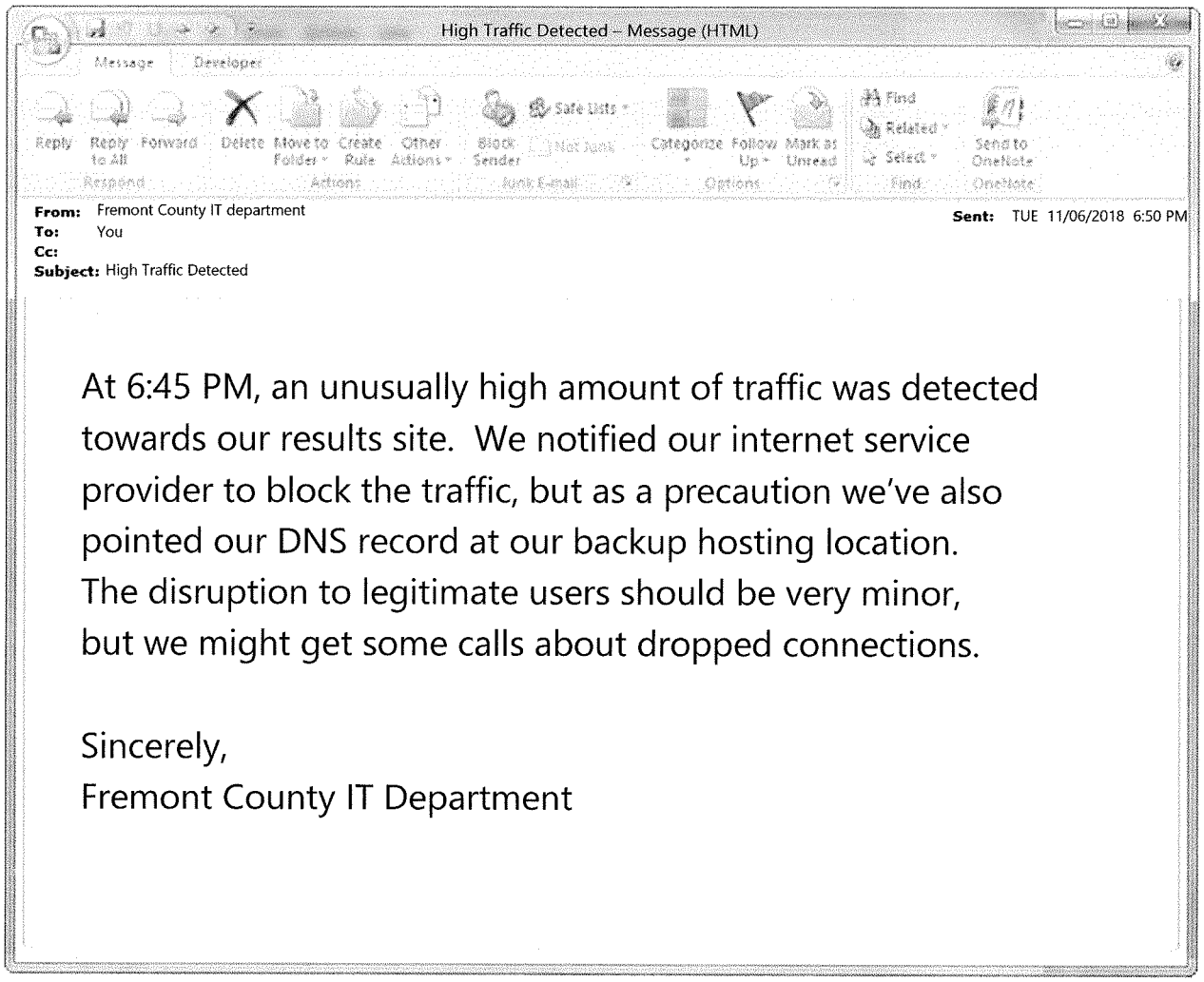
FLASH FLOODING IS EXPECTED TO BEGIN SHORTLY...

A FLASH FLOOD WARNING MEANS THAT FLOODING IS IMMINENT OR OCCURRING.
IF YOU ARE IN THE WARNED AREA MOVE TO HIGHER GROUND IMMEDIATELY.
RESIDENTS LIVING ALONG STREAMS AND CREEKS SHOULD TAKE IMMEDIATE
PRECAUTIONS TO PROTECT LIFE AND PROPERTY.

[As audio flood warning]

THE NATIONAL WEATHER SERVICE IN SULLIVAN HAS ISSUED A THUNDERSTORM WATCH FOR THE COUNTIES OF FREMONT, JAMESON, AND HARRISON COUNTIES... UNTIL 6:15 PM TUESDAY.

A Thunderstorm watch is issued by the National Weather Service when conditions are favorable for the development of severe thunderstorms in and close to the watch area.


High Traffic Detected – Message (HTML)
Message
Developer
Reply
Reply to All
Forward
Delete
Move to Folder
Create Rule
Other Actions
Block Sender
Safe Lists
Not Junk
Categorize
Follow Up
Mark as Unread
Find
Related
Select
Send to OneNote
Respond
Actions
Junk E-mail
Options
Find
OneNote
From: Fremont County IT department
To: You
Cc:
Subject: High Traffic Detected
Sent: TUE 11/06/2018 6:50 PM
At 6:45 PM, an unusually high amount of traffic was detected towards our results site. We notified our internet service provider to block the traffic, but as a precaution we've also pointed our DNS record at our backup hosting location. The disruption to legitimate users should be very minor, but we might get some calls about dropped connections.
Sincerely,
Fremont County IT Department

Is our election under attack? Car strikes polling place, "motive unclear"

By DYLAN SMITH NOVEMBER 6, 2018

At 4:28 PM a white Ford Explorer traveling east on Woodcock boulevard left the road at over 45 miles per hour and accelerated towards the Hancock Public Library where the line to vote was out the door. The vehicle sped towards the polling place, ramming through the waiting voters and into the wall of the library, causing significant damage. Witnesses say that at least 4 people are dead, and that as many as 15 more may be injured.

The driver, 57-year old Justin Rivers from Note Chez, Midlands, appears to have been killed in the collision. The FBI is handling the investigation and exploring possible ties to recent terrorist attacks such as the so-called "incel attack" that killed 10 in Toronto. Rivers, a white male, was a well-liked man, associates say, but a troubled one. He was receiving treatment for depression and anxiety. Friends say his health was a primary concern, as he was struggling to pay for the medications that controlled his diabetes and high blood pressure.

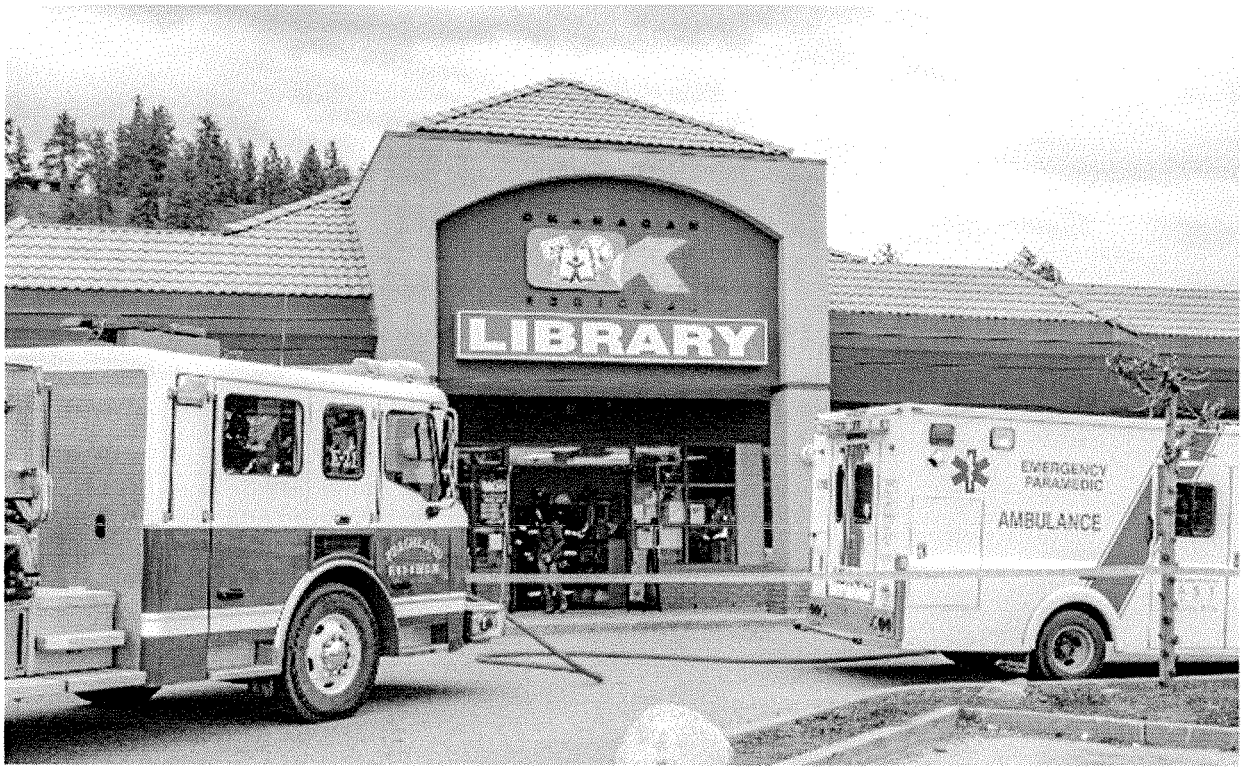
At this time, no motive for the attack has been revealed. A representative of the Freedom Party of Midlands has released a press statement announcing that "no amount of violence would keep Freedom voters from the polls."

Hancock polling place struck by vehicle: at least two dead, voters in disarray

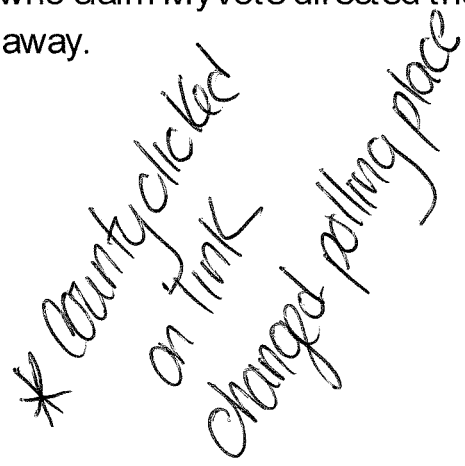
11 minutes ago

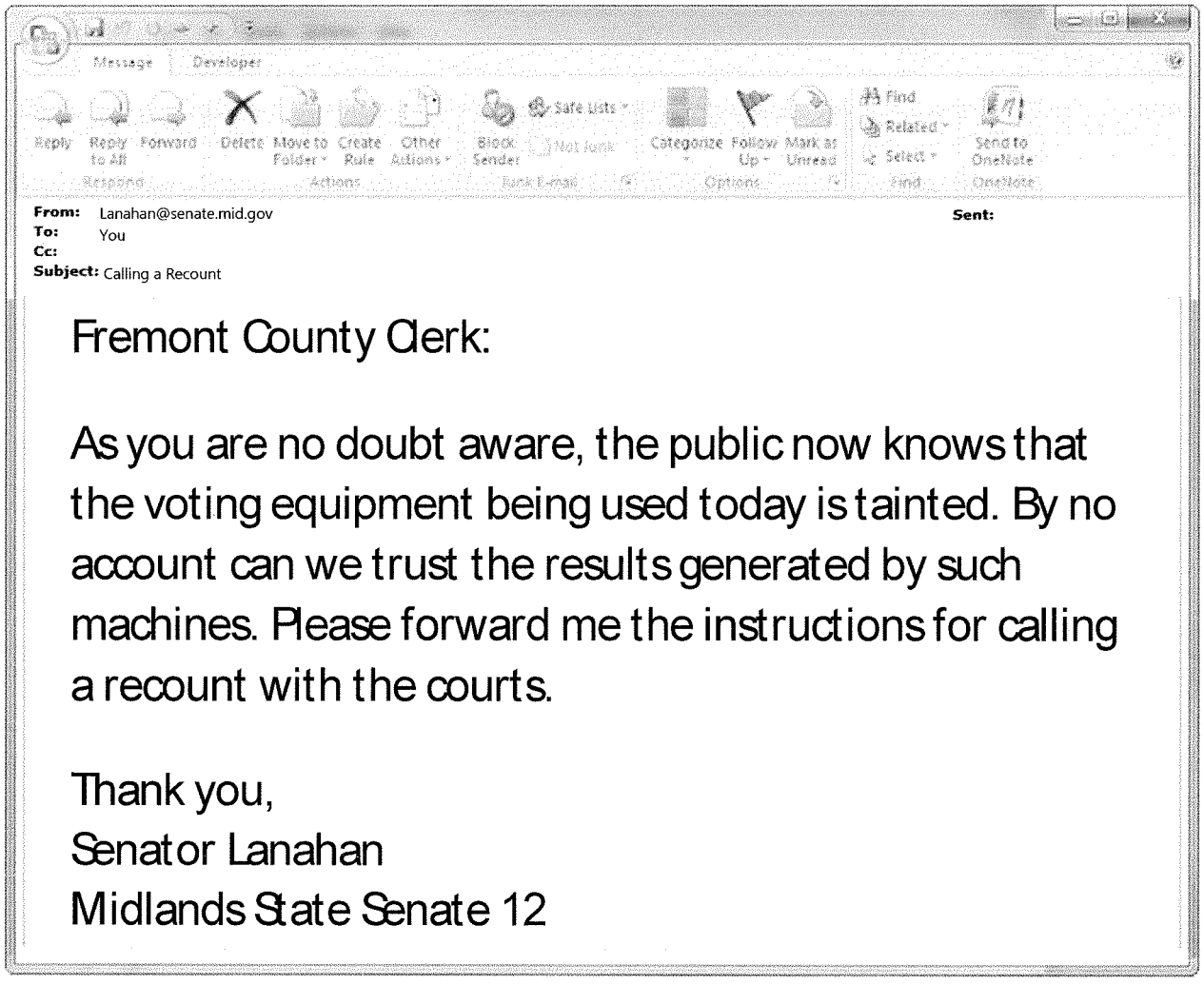
Share

Election 2018



You begin getting angry calls from voters who claim MyVote directed them to vote at Disney World, thousands of miles away.





Message | Developer

Reply | Reply to All | Forward | Delete | Move to Folder | Create Rule | Other Actions | Block Sender | Safe Lists | Not Junk | Categorize | Follow Up | Mark as Unread | Find | Related | Select | Send to OneNote

Respond | Actions | Junk E-mail | Options | Find | OneNote

From: Lanahan@senate.mid.gov **Sent:**
To: You
Cc:
Subject: Calling a Recount

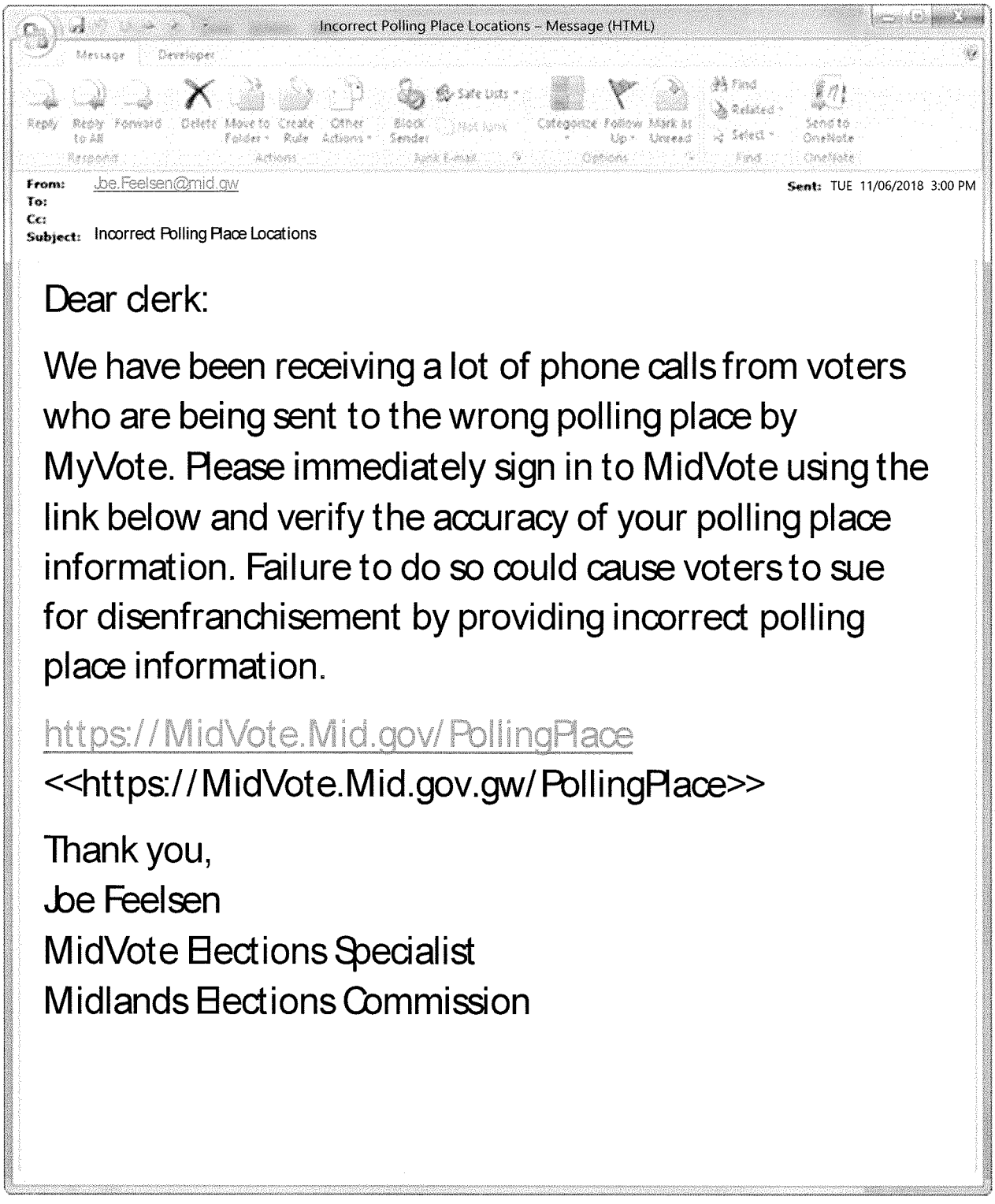
Fremont County Clerk:

As you are no doubt aware, the public now knows that the voting equipment being used today is tainted. By no account can we trust the results generated by such machines. Please forward me the instructions for calling a recount with the courts.

Thank you,
Senator Lanahan
Midlands State Senate 12

Calls begin to flood in demanding a hand count of today's vote.

A voter calls the county complaining about school children holding a bake sale in hallway outside room where voting is taking place, says some baked goods contain peanuts, which disenfranchise her.



Incorrect Polling Place Locations – Message (HTML)

Message Developer

Reply Reply to All Forward Delete Move to Folder Create Rule Other Actions Block Sender Safe Lists Not Junk Categorize Follow Up Mark as Unread Find Related Select Send to OneNote

Respond Actions Junk E-mail Options Find OneNote

From: Joe.Feelsen@mid.gw
To:
Cc:
Subject: Incorrect Polling Place Locations

Sent: TUE 11/06/2018 3:00 PM

Dear clerk:

We have been receiving a lot of phone calls from voters who are being sent to the wrong polling place by MyVote. Please immediately sign in to MidVote using the link below and verify the accuracy of your polling place information. Failure to do so could cause voters to sue for disenfranchisement by providing incorrect polling place information.

https://MidVote.Mid.gov/PollingPlace
<<https://MidVote.Mid.gov.gw/PollingPlace>>

Thank you,
Joe Feelsen
MidVote Elections Specialist
Midlands Elections Commission

Media:

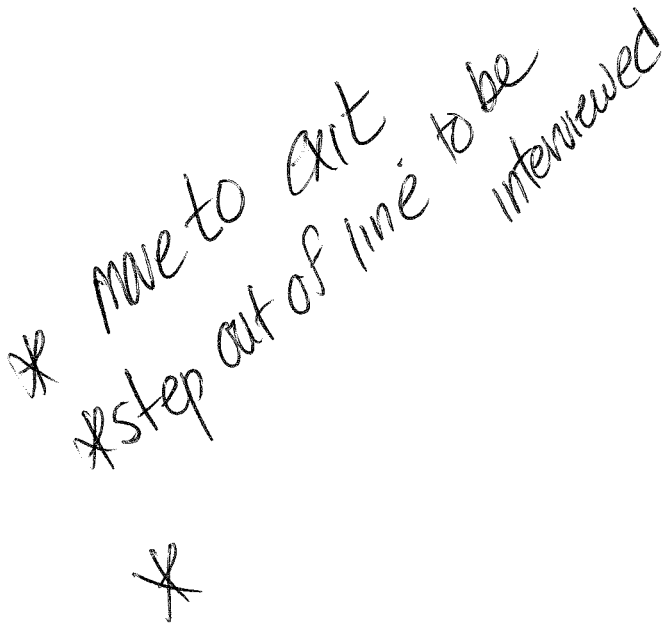
What do you have to say regarding the breach of Democracy Directive, your voting equipment programmer? Do you believe this breach impacts the security of the election? Do you intend to hand tally the vote?

Breaking News:
Attackers infiltrate elections programming

By DYLAN SMITH NOVEMBER 6, 2018

An anonymous source within Democracy Directive, the third-party vendor used by Fremont and Nicon Counties to program their election equipment, has revealed that their internal networks have been breached by an unknown assailant as many as 45 days ago. It is as yet unknown how much access this attacker had and what changes they might have made, but there is significant overlap between the time the breach is believed to have occurred and the time during which voting equipment was programmed for today's election.

A municipality calls about a cable network TV reporter and videographer showing up at polling place with a very long line and start interviewing voters live on air while they're waiting to vote.



Verbal: A caller is screaming about electioneering at her polling place, claiming that people are buying votes.

Moderator's note: The caller is complaining about a bake sale in the hallway.

*Will check into it -

* Catawba - city clerk OK

* State - Breach - deactivating - has EDR - reg + vote

An election inspector for a small town calls for guidance because an elector came in to vote but had already signed the poll book. Elector claims that he did not already vote and is furious that someone is stealing his vote. He has threatened to call the police and news media.

Moderator's note: The elector has the same name as his son. His son came in and voted, and signed on the wrong line.

Moderator Tips

This is a collection of tips, in no particular order, based on the experience of WEC moderators conducting the tabletop exercise for various groups around the state.

- Feel free to make up answers to small-scale questions about the scenario, such as the number of polling places in a municipality. Having a consistent answer throughout a simulation is more important than being "correct."
- Encourage participants to get up and talk to the participants at the other tables. If a participant says, "I would talk to the state," for example, encourage the participant to get up and walk over to the state table. This promotes keeping other participants at other tables involved in your decision making, as well as providing context clues to your own simulation.
- Try to get everyone involved. If a participant at a table is taking a back seat, start directing injects specifically to that person if it doesn't necessarily make sense. In the real world, it is not uncommon for emails and phone calls to end up where they do not belong.
- Fill in for the media. If there are no media moderators, or if the media moderators are busy elsewhere, you can fill that role by telling participants that a reporter is asking questions about an inject.
- Make sure everyone is having fun. Participants learn more and remember better when they are engaged. Make small-talk in between injections. Allow participants to make light of situations, so long as they also respond to them. Interrupt dull moments with flavor injects.
- Some participants may be reluctant to engage. If they are not responding to injects, put the pressure on them by saying that reporters are calling, or voters are threatening to sue.
- Allow for conversation. If there is debate about how to address an issue, let the participants come to their own solution even if you may disagree. This is their simulation, and any outstanding questions can be addressed in the TTX debrief.
- Feel free to talk to other moderators or the director of the TTX if you have any questions.
- Review the "flavor injects" before the start of the TTX and determine when you might want to incorporate them. While the "flavor injects" can be used in the TTX at any time, some might cause more debate than others, and it is good to be aware of the overall timeframe of your table.
- Flavor injects for counties and the state can, at the moderator's discretion, reference either a municipality that is being represented, or one that is not. In general, it is easier to reference an inject to a municipality that is not represented in the TTX than to try to coordinate flavor injects. In these cases, the discussion of that inject should take place amongst participants only at that table and the result of that discussion does not need to be communicated to participants at other tables. If a county moderator says an event happened at a municipality, but that municipality moderator has not drawn that inject, it causes confusion.

A municipality called to ask about a voter waving a "rare earth magnet" on a string around a tabulator.

You get calls about a man with a computer tablet with a long antenna who is travelling around the state, approaching poll workers, saying he has an app that can see hackers attacking the voting equipment via ultra-low frequency radio waves in real-time, and demanding polling place hand count all ballots.

Moderator's note: This person is mentally unstable. There is no threat from hackers, but the man may act unpredictably if confronted.

A voter calls complaining about pizza that was delivered to a polling place. The voter claims the pizza was a bribe by a candidate for sheriff.

A municipality calls and asks whether or not voters are allowed to take pictures of themselves with their ballot.

A municipality calls to request advice. A voter wearing a shirt that says, "If you don't vote, you can't squawk" brought a bird cage with a noisy parrot to the polling place. She claims the parrot is her service animal, and she's too nervous to vote without it. She refuses to leave until she can vote.

Multiple municipalities report 17-year olds attempting to register to vote. It seems like some confused pollworkers have allowed them to do so. They are carrying printouts from an online article.

A municipality calls to complain about a man demanding to see the tabulator seals and taking pictures of the polling place. He is carrying a shoulder bag with the old elections agency's name on it and says he was sent by the state.

Moderator's note: This is legitimate. The state should confirm that this is an accessibility auditor.

A voter calls because they needed to use the accessible voting equipment and it was not set up at their polling place.

Upset voters call regarding a car covered in political signs parked on the street outside the polling place. It is just over a hundred feet from the polling place entrance.

A caller reports a large number of voters getting out of a bus covered in candidate slogans. The bus has out-of-state plates.

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

INTERIM ADMINISTRATOR MEAGAN WOLFE

DATE: August 22, 2018

TO: Wisconsin County Clerks
Wisconsin Municipal Clerks
City of Milwaukee Election Commission
Milwaukee County Election Commission
Wisconsin Municipal Governing Bodies
Wisconsin County Boards

FROM: Meagan Wolfe
Interim Administrator, Wisconsin Elections Commission

Tony Bridges, Michelle R. Hawley, Riley Willman
Election Security Team, Wisconsin Elections Commission

SUBJECT: Election Security Awareness

The Wisconsin Elections Commission recognizes the importance of election security and how it is essential to administering elections that are free, fair, and efficient. With over 1,800 local election officials, Wisconsin has a unique election administration system whose success is dependent on cooperation between election partners from all levels of government. It is vital that all elected officials in the state continue to recognize the important role that safe and secure elections play in our state and support our local election officials in their duties of conducting and administrating elections in their communities.

In 2016, state computer systems were targeted by foreign actors in an attempt to access sensitive voter information housed in the WisVote voter registration database and election management system. Employees with the Department of Enterprise Technology quickly recognized the attempt and prevented any unauthorized access to voter information. The security threats that Wisconsin successfully prevented in 2016 will persist, and WEC staff are actively working to prevent any unauthorized attempts to access elections infrastructure in the future and to keep all aspects of election administration secure.

In March of 2018, the U.S. Congress allocated new Help America Vote Act (HAVA) grant funds to state elections agencies to be used to secure elections. Wisconsin was one of the grant recipients, and the WEC has used these funds to increase our election security efforts and upgrade information technology infrastructure to better prevent and detect threats. In addition to continuing the agency's previous tasks concerning election security, WEC staff has created a series of training videos to encourage cybersecurity best practices, published new manuals and documents to support clerks in implementing election security best practices in their offices, and created an interactive election security tabletop exercise program.

The election security training program that was created by WEC staff was conducted across the state for county clerks. In order to ensure that all local election officials and their staff have access to the security training, county clerks are currently conducting the training with their municipal clerks. A key aspect of the training was to gauge what various clerks were already doing to keep our elections secure, and many clerks have implemented some of the following best practices:

- Have voting equipment and associated memory devices stored in a secure and locked area between elections
    - Allowing only members of the clerk's staff to have access to these secure areas
    - Instituting a Chain of Custody document to show when and who accessed the secure areas
- Attend trainings to learn about new election security initiatives
- Secure additional access to IT resources or collaborate with existing IT resources to prevent cybersecurity incidents on the local level
- Coordinate with their emergency management teams to discuss contingency plans in the event of an election security incident
- Have updated technological resources (such as new computers, improved connections to the Internet, ability to get operating system updates and virus protection, etc.)

While clerks already have processes in place to keep our elections and their offices secure, many clerks also indicated that there was room for improvement. WEC staff recognizes that counties and municipalities have financial constraints that must be considered when making decisions regarding updating computer systems and purchasing other necessary resources to secure elections across the state. We would like to stress the importance of planning for election-related upgrades and encourage continued conversations with clerks about their resource needs.

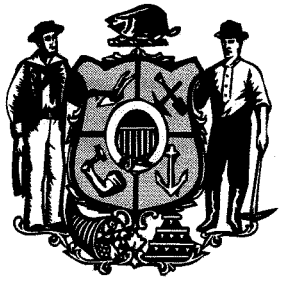
All elected officeholders in the State of Wisconsin benefit from the work and efforts of our local clerks and their staff. Wisconsin has a vested interest in making sure that they have the support and access to reasonable resources that they need. As the chief election officials in their areas, the county and municipal clerks of Wisconsin are a vital player in the administration of free, fair, secure and efficient elections. In order for these job duties to be performed, they require continued support from their governing bodies.

The Wisconsin Elections Commission would like to thank you for past support you have provided to your local election officials and encourage you to continue to work with your local elections officials to make sure that they have the tools and resources necessary to continue to keep our elections safe.

If you have any questions regarding the WEC's election security awareness program, please contact the Help Desk at 608-261-2028, or elections@wi.gov.

ELECTION SECURITY COMMUNICATIONS GUIDE

June 2018



Wisconsin Elections Commission
212 E Washington Avenue
P.O. Box 7984
Madison, WI 53701-2973
Phone: (608) 266-8005
FAX: (608) 267-0500
www.elections.wi.gov

How to Use this Communications Plan

The Wisconsin Elections Commission's communications plan includes guidelines and template materials to help election officials respond to an election-related security incident quickly and in a coordinated fashion during the first several days of a security incident. The Commission is indebted to the Harvard Kennedy School's Defending Digital Democracy playbooks, on which this plan is based.

While every situation is unique, this plan provides a foundation on which election officials can develop an appropriate response through different forms of media that address an incident with the goal of maintaining public confidence in the election system.

This plan will be updated on an annual basis, but more frequent updates may also be necessary.

Key components of this guide include:

- **Communications Process Workflow**: This component includes diagrams that outline who will manage crisis response, serve as spokesperson, and manage day-to-day crisis communications during an incident
- **Incident Best Practices**: This section includes best practices for communicating with the media and other key stakeholders.
- **Response Checklist:** This checklist broadly outlines steps that could be taken during the first several days after learning about a potential incident.
- **Scenario Planning and Materials**: This section will include communications materials that could be used in different scenarios, and includes potential resources in the event of an incident.

Establishing an Incident Response Workflow

To manage an election security incident effectively, the overall response to the incident should integrate communications officials from various levels of government into the process. The following organizational structure is designed to ensure that a communications plan is part of the decision-making process.

Incident Response Team Organization

Election security incident responses should use, to the degree possible, the already established processes in Wisconsin used to respond to other election-related issues. Responses should be adjusted to include specific information relating to the incident, but a response could be created from prior response materials or from the guides discussed in this manual. An incident response team should be formed that includes members who can assist in a variety of different capacities in the event of an elections security. Members can include existing clerk staff, legal counsel, public works employees, IT staff and other municipal employees or representatives, but a response team does not need to include representation from all of these groups. The team should be customized to fit the needs and resources of a specific county or municipality.

This table should be updated regularly as part of the annual plan review. If you do not have certain positions listed below in your office, designate someone from your office who could take on those roles in the event of an election security incident

State Contacts

Position	Designated Individual and Contact Information	Designated Backup and Contact Information
Wisconsin Elections Commission	Help Desk 608-261-2028	*WEC Administrator*
WEC Administrator	Meagan Wolfe 608-266-8175	*Assistant Administrator*
Assistant Administrator	Richard Rydecki 608-261-2015	*WEC Staff Counsel*
WEC Staff Counsel	Michael Haas 608-266-0136	*Public Information Officer*
Public Information Officer	Reid Magney 608-279-0477	

County Contacts

Position	Designated Individual and Contact Information	Designated Backup and Contact Information
County Clerk	Name: Phone Number	
Deputy Clerk	Name: Phone Number	
Public Information Officer	Name: Phone Number:	
Director of Operations and IT	Name: Phone Number	
Corporation Counsel	Name: Phone Number:	
District Attorney	Name: Phone Number:	

Municipal Contacts

Position	Designated Individual and Contact Information	Designated Backup and Contact Information
Municipal Clerk	Name: Phone Number:	
Deputy Clerk	Name: Phone Number	
Public Information Officer	Name: Phone Number:	
Director of Operations and IT	Name: Phone Number	
Municipal Attorney/Legal Counsel	Name: Phone Number	

Incident Communications Best Practices

The top priority during an election security incident is to maintain public trust through a swift and effective response that involves communicating relevant details about the incident to a variety of election partners and the public. The most effective way to achieve that goal is to respond confidently and quickly.

To lead confidently, election officials need to train for incident prevention and prepare and test responses ahead of time. In today's dynamic environment, every official will likely have to respond to an election security incident at some point. That response will be essential to preserving public trust.

Communications Coordination

- **Set guidelines for communicating with outside partners during an incident.**

  Election officials should create a communications plan that provides escalation thresholds for reporting an incident internally and publicly. The guidelines should also address who is responsible for communicating with key external stakeholders, such as other clerks in the area, the media, and law enforcement. It should also outline the timeframe for these communications and identify key individuals involved in communications response from the incident response team.

  Guidance on determining when and how to escalate an incident is available from the Wisconsin Elections Commission. As always, we are a resource for you to employ in the event of an election security incident and encourage you to contact our office if you have any questions or concerns about the severity of an incident.

- **Establish connections between the incident response team and communications officers.**

  Every situation will require collaboration and cooperation between multiple team members and other individuals or groups involved in developing an appropriate and effective response. Well-developed relationships between the incident response team and other response partners create credibility that is vital to a successful post- incident recovery.

- **Encourage intra-state, cross-state, or cross-country communication and collaboration.**

  Key organizations to designate for regular communications include: the Wisconsin Elections Commission, as well as county and municipal clerks. If necessary, the WEC will contact state and federal leaders, such as the Department of Homeland Security, the Federal Bureau of Investigation or other Wisconsin state agencies that oversee state information technology infrastructure. Develop good working relationships between your municipality/county and other key election officials and maintain an updated contact list of these individuals for use during an incident.

Planning Ahead

Near-term Planning

- **Determine internal roles and responsibilities.** Make sure there is a clear escalation process within your municipality/county and the right teams are talking to one another in the event of an incident. Designate an individual to be responsible for ensuring that this process is established and updated.
- **Assess the current crisis communications plan** to identify communications gaps and weaknesses that need to be addressed.
- **Plan your response to a potential incident in advance** with a communications plan, including a decision-making protocol and draft communications materials.
- **Ensure incident response is part of the operational continuity plan.** Make sure there is a backup communications plan and system in place.

Longer-term Planning

- **Conduct crisis simulation and table-top exercises**, coordinated with internal clerk staff, legal, technical, and outside advisors.
- **Educate the media** through background meetings and public events that focus on the resiliency of the election system, and the current work being done to prevent and address threats.
- **Educate the public** through social media and public events that focus on the resiliency of the election system and the current work being done to prevent and address threats. Occasionally members of the public can get misinformation about election security and administration specifically in Wisconsin, and it is important to frequently dispel rumors and show the public what your office is doing to maintain Wisconsin's secure elections.

Communications Response

Best Practices

- **Coordinate with the Wisconsin Elections Commission beforehand** and discuss how the WEC should be involved with timely incident response.
- **Respond to the incident in a timely fashion.** While it is important to coordinate with members of your incident response team before communicating with media or the general public, it is also important to communicate your message in the moments after an election security incident.
- **Be transparent but careful**. Transparent communication builds trust, but in a security incident you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously, but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator/cause of the incident.

- **Focus on actions you are taking to address the issue.** To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and other election resources, such as ballots and voting equipment, and address any broader risks to the system.
- **Provide context**. In an election security incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include facts/figures or concrete steps that are being used to address the issue whenever possible.
- **Speak plainly**. Election security, especially cybersecurity, can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify relevant issues whenever possible.
- **Use the right digital tools**. Use social media to dispel rumors. When an incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation and inaccuracies. Even if you do not use social media on a frequent basis, it is a good idea to have an official account for your office, and to be in contact with other officials in your community who could also spread your message through their own official social media accounts.
- **Learn from the incident**. Use your and others' experiences to improve your security practices and crisis plans. Conduct an after-action briefing to evaluate the response and identify aspects that were effective and suggest improvements.

Guidelines for Communicating with the Public

- **Make your communications about the public**. There will be a temptation for you to focus your communication on the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this specific situation.
- **Demonstrate transparency by communicating with the public on a regular basis before a potential incident occurs**. Establish a regular series of communications with the media and the public about the security measures you are taking now, so that the first time they hear from you is not in a crisis.
- **Understand what requires an official response.** Sometimes questions about incidents do not require an official public response, and can be handled by simply providing an answer directly to the individual with the question.

Best Practices for Countering Misinformation

- **Establish the facts, and double-check them**. You need to ensure you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to ensure that you do not accidentally provide misleading information.

- **Develop a simple, accurate, short counter-message**. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later if needed.
- **Respond quickly**. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready to disseminate as soon as possible.
- **Be transparent**. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Demonstrating transparency can help counter false claims and prevent misinformation from spreading. Engage in opportunities to demonstrate transparency by potentially inviting reporters "behind the scenes" at a polling place, or providing frequent press updates about the work being done to resolve the incident.
- **Engage on all platforms**. Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms, and consult with other local government and election partners to help deliver that same message.
- **Avoid repeating misinformation**. Focus on providing a positive response based on accurate facts and do not repeat any false messages or rumors. For example, if rumors circulate that lines at the polls are hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

Developing a Response Process and Checklist

The following steps will guide you as you organize an Election Security Communications Response Team and develop a process for drafting and approving messages.

- **Step 1: Decide on team**. Select the individual(s) who will fill the roles previously listed. Outline their roles and identify the decisions around messaging and communication that they can make in real time.
- **Step 2: Security alignment**. With your team, take inventory of your assets and potential risks, and conduct an impact assessment. You should understand the attacks to which you are most vulnerable. You should also understand how security tactics are tied to the way your election office manages risk. Your team's early monitoring and detection functions should be aligned to the agency's most critical assets, such as ballots, ballot boxes, voting equipment, computers with WisVote access, etc.
- **Step 3: Disclosure alignment**. Determine and document exactly what you are obligated to disclose. Develop a decision-making process to assess the public posture—proactive or reactive—you will take in a given situation. Consider both legal implications and public opinion. Consult with your municipal attorney, county or the WEC if you have questions on what to/what not to disclose.

Developing a Response Process and Checklist

The following steps will guide you as you organize an Election Security Communications Response Team and develop a process for drafting and approving messages.

- **Step 1: Decide on team**. Select the individual(s) who will fill the roles previously listed. Outline their roles and identify the decisions around messaging and communication that they can make in real time.
- **Step 2: Security alignment**. With your team, take inventory of your assets and potential risks, and conduct an impact assessment. You should understand the attacks to which you are most vulnerable. You should also understand how security tactics are tied to the way your election office manages risk. Your team's early monitoring and detection functions should be aligned to the agency's most critical assets, such as ballots, ballot boxes, voting equipment, computers with WisVote access, etc.
- **Step 3: Disclosure alignment**. Determine and document exactly what you are obligated to disclose. Develop a decision-making process to assess the public posture—proactive or reactive—you will take in a given situation. Take into account both legal implications and public opinion. Consult with your municipal attorney, county or the WEC if you have questions on what to/what not to disclose.
- **Step 4: Stakeholder analysis**. Assess and prioritize your key stakeholders, based on their influence on voters, because public opinion can turn very quickly during a security crisis.
    - Establish ongoing relationships with these stakeholders BEFORE a crisis hits. Your stakeholders may include:
        - Voters
        - Federal, state, and local election communications counterparts
        - Law enforcement
        - State and federal lawmakers, including the Wisconsin Elections Commission
    - Media (local media, cybersecurity and election/political beat reporters)
    - Political parties and campaigns
- **Step 5: Determine a spokesperson**. Establish ahead of time who will speak for your office during an election security incident. You may choose different spokespeople for different audiences. Your head of IT might be best equipped to post a response concerning a cybersecurity incident, while the county or municipal clerk might be the best person to speak to the media. You can also always consult the WEC to handle media requests. Consider factors such as who has the best communication skills, prior experience with the media, authority in the agency, and relationships with stakeholders.
- **Step 6: Establish a drafting and approval process for key messages and include diagrams of this process in your communications plan.** This process will be specific to your team's structure.

- **Step 7: Decide what baseline information you can communicate now**. Establish a baseline understanding among key stakeholders of your county's/municipality's work to implement security best practices well ahead of the next election. In the event of an incident, this effort will position you to make the case that you have been implementing best practices, but unfortunately incidents do still sometimes occur.
- **Step 8: Establish a feedback loop.** Establish a means — both during and after an incident— to incorporate feedback from voters and other key stakeholders into your response. During an incident, this work could take the form of media and social media monitoring as well as informal polling. After an incident, you should conduct an after-action report and ensure that lessons learned are incorporated into this communications plan template. Your after-action report should include:
    - A summary of the incident (keeping in mind it could be subject to public disclosure);
    - an overview of the operational response;
    - the communications objectives;
    - outcome and future recommendations

Sample Scenarios and News Release Examples

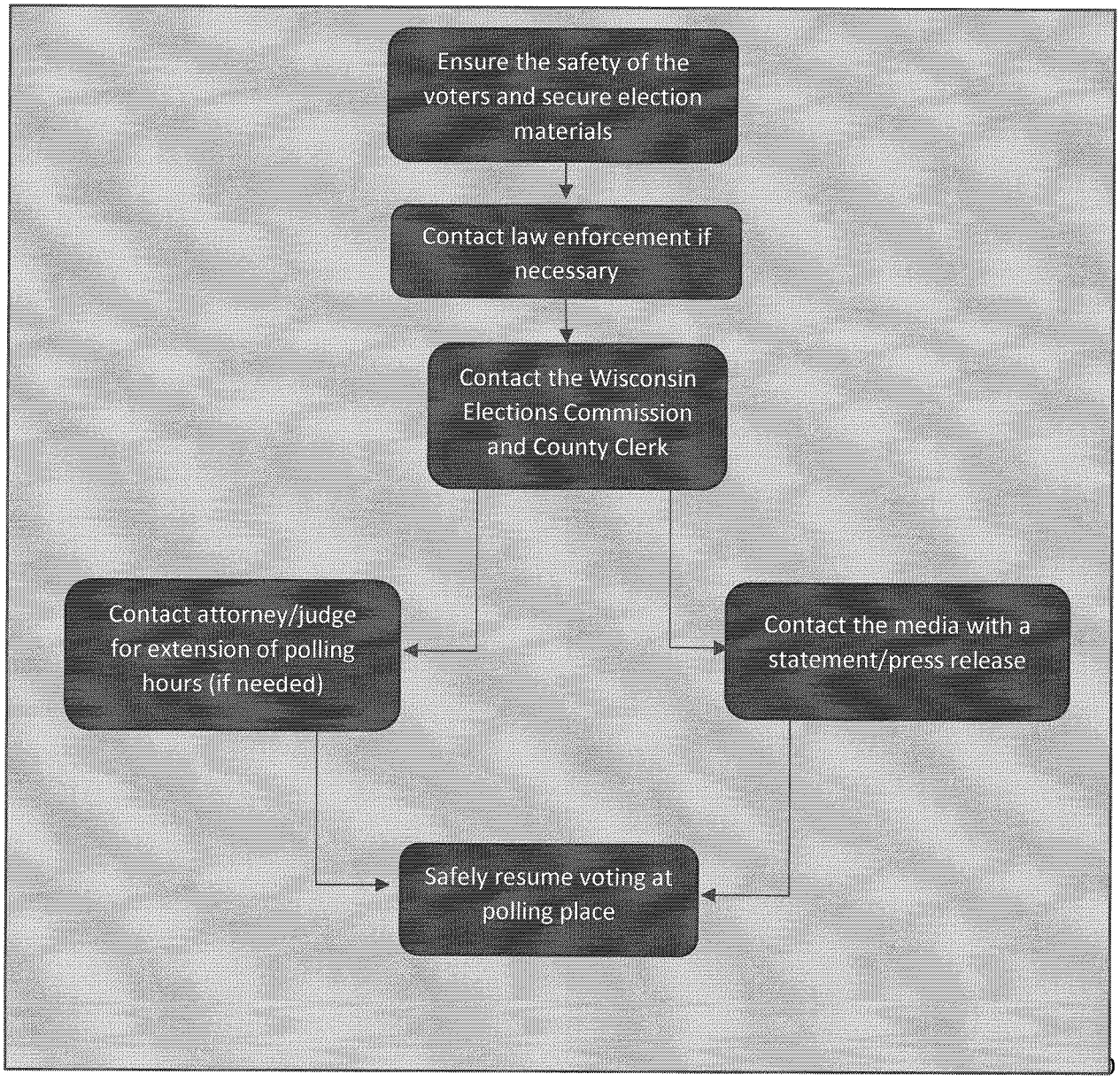
To help illustrate what the flow of communication could look like in the event of an election security incident, we have outlined some potential situations that could occur in the time before and on Election Day. Please note, every incident and response will be different, and these communication tools will have to be customized to fit your needs and the situation. As always, you can consult the WEC if you have any questions on communicating a security incident.

Scenario One

Time: Morning of Election Day

Location: A polling place

Issue: Your polling place is temporarily inaccessible.

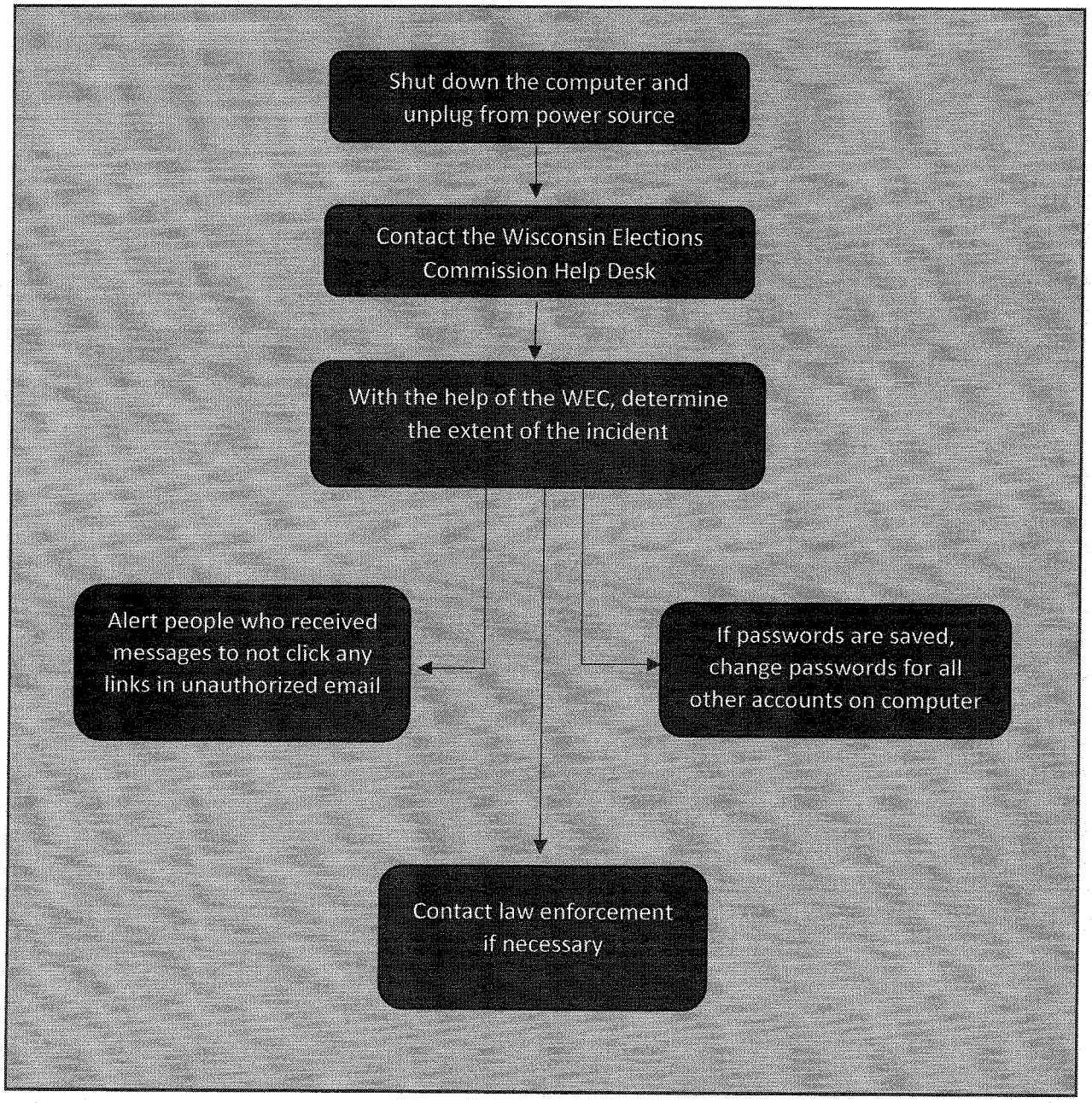


Scenario Two

Time: One Month Before Election Day

Location: Your Office

Issue: A member of your staff accidentally clicks on an email attachment from an unknown sender and starts sending out unauthorized emails. This is an office computer, and is logged in to WisVote at the time.

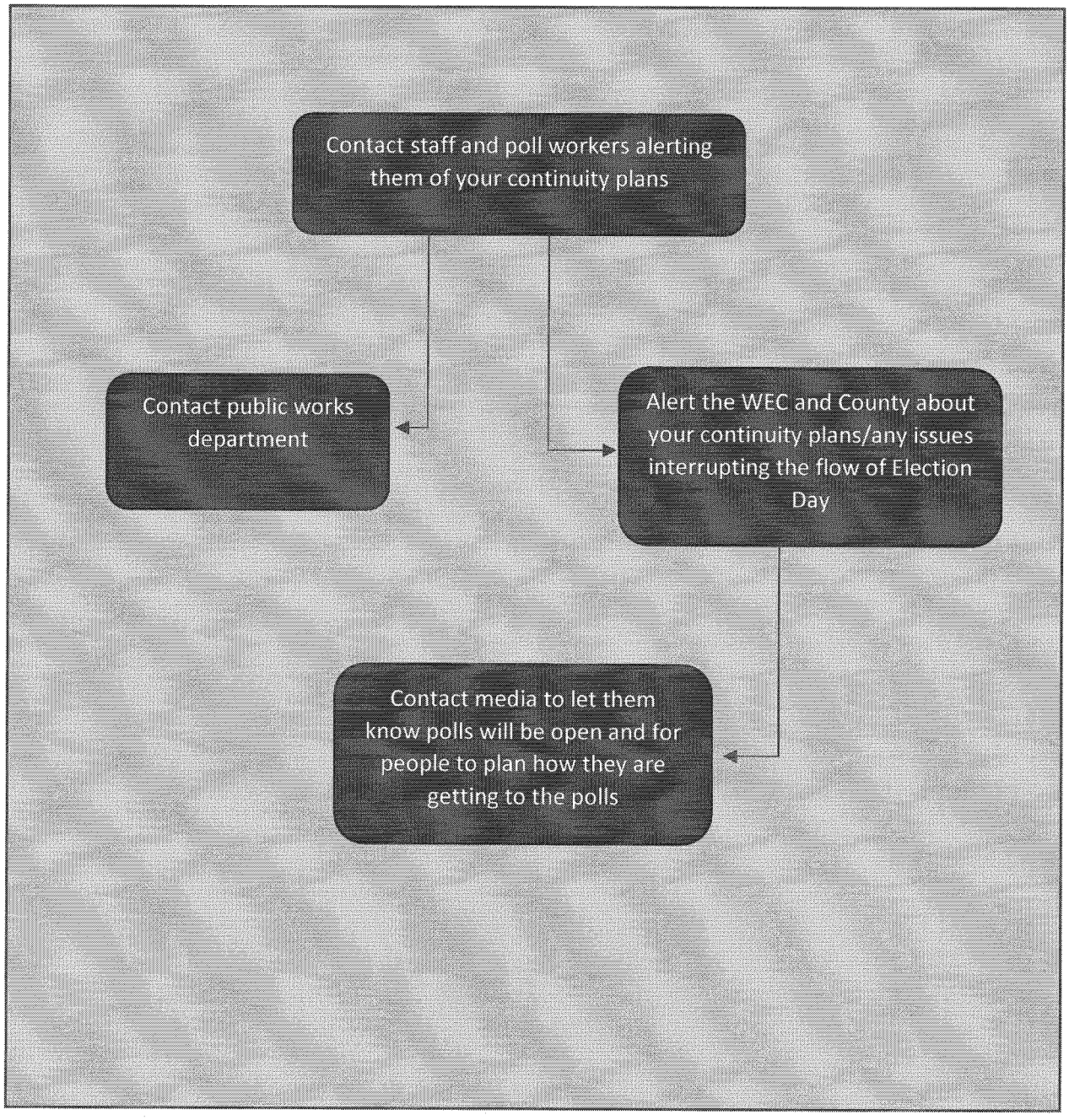


Scenario Three

Time: One Day Before Election Day

Location: Your Office

Issue: You are preparing for Election Day, and learn that there are going to be severe storms in the area all day tomorrow, potentially making the polling place inaccessible all day.



Sample News Release - Weather

August 12, 2018

FOR IMMEDIATE RELEASE

CONTACT: Cheddar County Clerk Jane Smith, 715-555-1212, jane.smith@cheddarcounty.gov

Polling Place Affected by Flooding

TOWN OF EAST OVERSHOE, Wis. – Voters in the Town of East Overshoe will have to vote at the Overshoe Middle School on Tuesday, August 14 due to flooding, according to County Clerk Jane Smith.

Rising floodwaters from the Little Cheddar River will likely make County Highway 13 and Town Road Z impassible by Tuesday, cutting off vehicle access to the East Overshoe Town Hall, Smith said.

"After meeting with East Overshoe Town Clerk Roberta Jones, Town Chair Jim Johnson, Overshoe School District Superintendent Bruce Benson, West Overshoe City Clerk Cindy Larson and Cheddar County Emergency Management officials, we determined it would be best to move the polling place to higher ground," Smith said. "We also consulted with the Wisconsin Elections Commission."

"The Overshoe School District has kindly offered to let us use the Library Media Center at the Middle School for a polling place on Tuesday," said Clerk Jones. Town voters should enter through the main entrance and follow the signs.

City of West Overshoe voters will continue to vote in the Gymnasium, and should use the entrance by the football field, said Clerk Larson.

Clerk Jones said East Overshoe town workers will be stationed at Highway 13 and Road Z, and will have maps showing the route to Overshoe Middle School.

Town crews have already moved voting equipment and election supplies from the Town Hall to the Middle School, where it is being kept in a secure location until Election Day, Clerk Jones said.

Town of East Overshoe Voters who have questions should call Clerk Jones at 715-555-3456.

Sample News Release – Cyber Incident Rumors

October 24, 2018

FOR IMMEDIATE RELEASE

CONTACT: East Overshoe Town Clerk Roberta Jones, 715-555-3456.
Roberta.Jones@townofeastovershoe.org

East Overshoe Voting Equipment Safe and Secure

TOWN OF EAST OVERSHOE, Wis. – Town Clerk Roberta Jones said today she is confident that the town's voting equipment is secure and that voters can trust the results when they are tabulated on November 6.

"Shortly after the August Partisan Primary, there were concerns about a problem with our voting equipment because the ballot scanner jammed on Election Day and took longer to fix than normal," Jones said.

"The problem was entirely mechanical, and was not caused by online hacking," Jones said. "It took longer than expected to fix because the repair person was delayed due to vehicle problems."

Since August, Cheddar County Clerk Jane Smith has replaced the old scanner with reconditioned model, which has been tested for logic and accuracy.

On 10 a.m. on October 29, the Town of East Overshoe will conduct a public test of the voting equipment at the Town Hall to ensure it can performed its tasks accurately, Jones said. "Any member of the public is welcome to attend the public test," she said.

"None of the Town of East Overshoe or Cheddar County's voting equipment is connected to the Internet," Smith said. "The computer my office uses to program Cheddar County's voting equipment is hardened, meaning it is not connected to the county's internal network, and is not used for any other purpose." She said Cheddar County's Information Technology Department regularly scans the computer for viruses and other malware.

Jones said anyone who wants to observe the vote counting on Election Night and hear the unofficial results when they are announced is welcome to come to the East Overshoe Town Hall at 8 p.m. Results will be posted on the Cheddar County Clerk's website later in the evening: https://elections.cheddar.co.wi.us.

Town of East Overshoe Voters who have questions should call Clerk Jones at 715-555-3456.

Sample News Release – Equipment Malfunction

August 14, 2018

FOR IMMEDIATE RELEASE

CONTACT: East Overshoe Town Clerk Roberta Jones, 715-555-3456.
Roberta.Jones@townofeastovershoe.org

Voting Equipment Malfunctions, Elections Continue

TOWN OF EAST OVERSHOE, Wis. – A ballot scanner in the Town of East Overshoe jammed early today and is taking longer than anticipated to fix, according to Town Clerk Roberta Jones.

"I immediately contacted Vote-O-Matic to send a repair person, but the repair truck got stuck in a ditch outside Eau Claire when it swerved to avoid hitting a deer. Luckily nobody was hurt, but the repair person will not be here until late this afternoon," Jones said.

Until then, voters will deposit their marked ballots for today's Partisan Primary in a secure, auxiliary ballot box, which will remain locked until the voting equipment is repaired. When the scanner is ready, poll workers from both political parties will open the ballot box and begin tabulating ballots, Jones said.

The delay in repairing the ballot scanner may cause delays in reporting unofficial results to the Cheddar County Clerk's Office after the polls close.

Jones said anyone who wants to observe the vote counting and hear the unofficial results when they are announced is welcome to come to the East Overshoe Town Hall at 8 p.m. Results will be posted on the Cheddar County Clerk's website later in the evening: https://elections.cheddar.co.wi.us.

Town of East Overshoe Voters who have questions should call Clerk Jones at 715-555-3456. Periodic updates will also be posted on the town's Twitter page: https://twitter.com/eastovershoe

Attached please find an Election Day Emergency Response Plan template that can be used to create a contingency plan to prepare for challenging or emergency situations on Election Day. One of the big take-aways from conducting election security training and tabletop exercises was that some municipalities and/or counties do not currently have an emergency response plan, or that existing plans were out of date. As a result, the Wisconsin Election Commission created this template to aid in drafting a plan for your community to ensure that each municipality and county have a current and updated plan.

This document is intended to be a template and is available to you in Word format, on the WEC Learning Center, so that you may create a customized plan that reflects your situation and resources. We have provided scenarios and some suggested responses and encourage you to edit and tailor the document to meet your needs. For example, there are general references to voting equipment. There are many different types of equipment and vendors used throughout the state, so we strongly suggest and encourage you to contact your specific vendor to verify how your equipment works if, for instance, should the power have to be temporarily turned off in an evacuation situation or should you lose power at a polling place on Election Day.

As always, should you have any questions or concerns, please feel free to reach out to our office.

Thank you,
Elections Security Team
Wisconsin Elections Commission
July 2018

P.S. Don't forget to delete this page and remove the "template" watermark to your final draft.

(INSERT NAME OF COMMUNITY)
ELECTION DAY EMERGENCY RESPONSE PLAN

This document is maintained by:

(Enter who and where (file path) maintained)

Last updated: _____

TABLE OF CONTENTS

INTRODUCTION

Purpose:

This document will serve as the emergency response/contingency plan in case of an unexpected circumstance that requires a change in the standard operating procedures on Election Day. The purpose of this document is to provide guidance for election staff and for the general safety of polling locations, all while maintaining the integrity of an election.

This document shall be reviewed with Election Inspectors as part of the Clerk's pre-election training. The document and its contents shall be considered sensitive in nature. County Clerks, as well as polling place property owners and facility managers, should be apprised of relevant aspects of these plans.

Polling Place Staffing, Hours of Operation, and Location(s)

Address of this Polling Location:

_____

_____

_____

Staffing:

This polling locations will have the following staff on site:

- Chief Election Inspector (1-3)
- Election Inspectors (10-12)

Hours of Operation:

Voters may cast their ballots from 7:00 a.m. to 8:00 p.m.

Extended Polling Place Hours:

In the event of an emergency, a court order may be requested to extend polling place hours.

EMERGENCY PROCEDURES

Chief Election Inspectors should ensure that Election Inspectors are made aware of these procedures and their responsibilities in advance of an election, if possible. Identifying duties and assigning them in advance may help alleviate stress and clarify responsibilities in case of an emergency.

A. WORLDWIDE TERRORISM EVENT

In the event of terrorist activity, the Federal Government may have a preliminary plan in place for moving activities on election days. All elections will continue unless Federal or State officials have ordered otherwise. If there are no police orders to take cover or to remain indoors, all operations of polling places can remain intact. If you are notified to evacuate the polling place, follow the instruction regarding evacuation in this plan (see Section E. Evacuation).

B. ACTIVE SHOOTER

Active shooter situations are unpredictable and evolve quickly. As a result, these situations may be over even before law enforcement arrives on the scene. Individuals must be prepared, both mentally and physically, to react to an active shooter situation. U.S. Department of Homeland Security recommends these best practices when coping with an active shooter situation:

- Be aware of your environment and any possible dangers.
- Take note of the two nearest exits in any facility you visit or are assigned to work as an Election Inspector.
- If you are in an office, stay there and secure the door.
- If you are in a hallway, get into a room and secure the door.
- As a last resort, attempt to take the active shooter down. When the shooter is in close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her.
- Dial 9-1-1 WHEN IT IS SAFE TO DO SO!

C. WORKPLACE VIOLENCE / OTHER ACTS OF VIOLENCE

Be aware of the possibility of an incident occurring at your voting location. Treat all threats and warnings seriously.

- Report any and all threats to the Chief Election Inspector to make a determination as to the next course of action.

- **If a situation involves an immediate threat of violence to persons and/or the election process, dial 9-1-1.**
- In the event of a personal confrontation, do your best to stay calm.

D. THREATENING PHONE CALL/BOMB THREAT/SUSPICIOUS OBJECT

If you receive a written threat, suspicious package, or find a suspicious object on the premises:

- Keep anyone from handling or going near the object in question as it may be dangerous. (In addition, preservation of evidence is important for law enforcement).
- Stay calm and dial 9-1-1.
- Promptly write down everything you can remember about receiving the threat and/or finding/receiving the suspicions object.
- Depending on where the object is found (and in accordance with instructions from 9-1-1 operator/law enforcement), you may need to evacuate the polling place. If you are notified to evacuate the polling place, follow the instruction regarding evacuation in this plan (see Section E. Evacuation).

E. EVACUATION

Treat all threats and warnings seriously. If an evacuation becomes necessary (i.e., fire, fire alarm, etc.), the following steps can help keep people safe and effectively continue the election processes:

- Stay calm and dial 9-1-1.
- The evacuation and safety of human life is the first concern. Inform any voters at your location of the safety evacuation route.
- Secure election materials, if possible (voting equipment, ballots, inspectors' statements).
- Proceed to the designated area **(enter the pre-determined designated area for THIS polling place)** until/unless you are directed to do otherwise.
- Take accountability and note any missing people. Report missing people to emergency personnel.
- Stay in designated area until you are otherwise directed.
- Do not re-enter the building until authorized by emergency personnel.
- Do not speak to the media – refer them to the Chief Inspector or emergency personnel.

F. SEVERE WEATHER/NATURAL DISASTER

To ensure safety and security during inclement weather, the Clerk shall monitor and be in communication with local law enforcement, emergency responders, and Chief Election Inspectors. Safety of human life is the first concern.

- If a natural disaster occurs that provides ample time and requires inspectors and voters to take cover in the designated area **(enter the pre-determined designated area for THIS polling place)**, all unvoted ballots and polls lists will be secured by the Chief Inspector. The voting equipment/ballot box can be unplugged and locked in a secure storage area. No ballots shall be inserted into the voting equipment/ballot box, nor should any additional ballots be issued during this time. When regular business resumes, the Chief Inspector shall note the time from beginning to end that voting was suspended on the Inspectors' Statement.
- If a tornado is reported or seen in the immediate area, seek shelter in the designated area **(enter the designated area for THIS polling place)**. If time does not allow you to evacuate to a safe location, find shelter under a heavy object such as a table and protect your head.
    - Do not stop for personal belongings, ballots, or election equipment.
    - Take accountability and note any missing people.
    - If the building is struck by a tornado, remain in your location until it is safe to evacuate.
    - Stay away from sources of power, power lines, phone lines, gas lines, and windows.
    - Once you are clear of the area, do not re-enter the building until/unless authorized by emergency personnel.
    - Report missing people to emergency personnel.

G. ELECTRICAL OUTAGE

In the event a polling location loses power, voting equipment contains power supply backups that allow the equipment to continue to operate for approximately 3-4 hours. This battery backup also stores the totals for ballots already recorded.

Turn off the voting equipment and have voters deposit their ballots into the equipment's auxiliary compartment. Note the time of the power outage on the Inspectors' Statement and contact the clerk immediately. If flashlights and/or emergency lighting are not already available at the polling location, clerks should reach out to the **(department of public works and/or emergency management services – enter department or resources you can reach out to in case of this emergency)** to deliver flashlights and any other necessary supplies.

When power is restored, turn the voting equipment back on and process any voted ballots located in the auxiliary compartment through the equipment. If power is not restored before the end of Election Day, secure all voted ballots in a ballot bag and bring them, along with all of the election supplies, to the alternate location **(list alternate location here)**. Ballots will be processed at the alternate location.

In the event of a long-term power outage, a change of venue may be required (see Change of Polling Location, page 8). If there is a wide spread power outage, ballots should be secured with the Election Inspectors at the polling location until 8:00 p.m. In addition to the instructions listed above:

- Stay calm.
- Provide assistance to visitors and staff in our immediate area.
- If emergency lighting is available, proceed with caution to the area with lighting (perhaps this may be natural light from windows).
- Turn off the voting equipment. The tabulator memory device will retain all data in its memory and can be restarted after a power outage.

H. MEDICAL EMERGENCIES

If you observe a staff member or visitor who appears to be seriously ill or injured:

- Stay calm and dial 9-1-1.
  - Provide your location **(enter address of polling location or refer to page 2)** and the nature of the emergency.
  - Answer all questions asked by the 9-1-1 operator.
  - Listen to and follow all instructions provided by the 9-1-1 operator.
- Do not move a person who has fallen.
- Unless it is a life-threatening emergency, do not render first aid until a qualified individual arrives or you are instructed to do so by the 9-1-1 operator.
- If possible, try to obtain from the injured person his/her name and what happened.
- Report any injury to the clerk (after the injured person is safe).
- Avoid unnecessary conversation about the ill or injured person.
- Do not speak to the media – refer them to the Chief Inspector or emergency personnel.

CHANGE OF VENUE (POLLING PLACE)

When it has been determined by the Chief Election Inspector (in consultation with the Clerk and emergency management personnel, if applicable), that a polling location needs to be moved to effectively respond to a disaster/emergency, follow this guidance:

- The Election Inspectors will assist in packing up all voting equipment, ballots, poll lists, registration materials, and all election forms and information that needs to be relocated (e.g., signs, notices, etc.).
- The Clerk will organize transport vehicles and report to the polling location to help facilitate the move.
- All Election Inspectors will assist the Clerk in moving the election materials/equipment to the transport vehicles.
- The voting equipment/ballot box(es) will remain locked at all times.
- The voting equipment/ballot box(es) will be escorted to a municipal vehicle or police vehicle, if available. A police officer will remain in view of the voting equipment/ballot box(es) at all times and take them to the Alternate Location **(enter address of alternate location)**. At this location, the polling place will be set up as normal.
- All unvoted ballots should remain in the presence of the Chief Inspector and at least one other Election Inspector during the change of location.
- A sign should be posted on the front entry doors of the original polling location designating the new polling place (if the building is safe), or at a place as close to the entry doors as possible.
- A law enforcement officer, or another designated person will remain at the original polling location to direct voters to the new location.
- Notice should be provided/posted to the municipal website, local Public Access Channel, local radio, social media, etc. to direct voters to the new location.
- Notice should be provided to the Wisconsin Elections Commission.
- Inspectors should document the change of venue and what time voting resumed on the Inspectors' Statement.
- Does the situation warrant an extension of polling place hours?

EMERGENCY CONTACTS

Listed below are potential Election Day emergency contacts **(be sure to list both daytime and after hours phone numbers for these contacts and to update this list at least once per year).**

Municipal Contacts

Clerk	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Deputy Clerk	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Fire/Police/EMS	9-1-1
Fire/Police/EMS (non-emergency)	
IT Support	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Voting Equipment Support	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Municipal Attorney	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Public Works Department	Name:
	Daytime Phone Number:
	After Hours Phone Number:

County Contacts

Clerk	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Deputy Clerk	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Fire/Police/EMS	9-1-1
Fire/Police/EMS (non-emergency)	
IT Support	Name:
	Daytime Phone Number:
	After Hours Phone Number:
Voting Equipment Support	Name:
	Daytime Phone Number:
	After Hours Phone Number:
County Attorney	Name:
	Daytime Phone Number:
	After Hours Phone Number:
County Judge (on-call for election night)	Name:
(this will vary for every election)	Daytime Phone Number:
	After Hours Phone Number:
Public Works Department	Name:
	Daytime Phone Number:
	After Hours Phone Number:

State Contacts

Wisconsin Elections Commission	Help Desk: 608-261-2028
	Help Desk Email: elections@wi.gov
	For extended office hours and applicable phone numbers during those hours, please check **Recent Clerk Communications** tab the agency website (https://elections.wi.gov).
	Meagan Wolfe (WEC Administrator)
	Daytime Phone Number: 608-266-8175
	After Hours Phone Number: 608-712-6957
	Richard Rydecki (WEC Deputy Administrator)
	Daytime Phone Number: 608-261-2015
	Reid Magney (Public Information Officer)
	Daytime Phone Number: 608-267-7887
	Mike Haas (Staff Counsel)
	Daytime Phone Number: 608-266-0136

ELECTION SECURITY TRAINING AND TABLETOP EXERCISE (TTX)

WISCONSIN ELECTIONS COMMISSION

JUNE 2018

1

BACKGROUND

- **Defending Digital Democracy Project**
  Belfer Center for Science and International Affairs
  Harvard Kennedy School
- Decision to implement similar model in Wisconsin
- Survey to County Clerks
- Regional Train-the-Trainer Events

2

WHAT IS A TABLETOP EXERCISE (TTX)?

- Training simulation that:
  - Mirrors real world conditions
  - Assigns participants a role with corresponding responsibilities
  - Uses an accelerated timeline
  - Provides participants opportunity to experience scenario, make educated decisions, and execute plans

3

WHAT DOES THAT MEAN FOR YOU?

- Simulation of a very bad Election Day (this should be challenging to get you thinking . . . always room to learn more about keeping elections safe)!
- Desired outcome:
  - Assess effectiveness of existing knowledge, policies, and practices as they relate to election security (operational, physical, cyber)
  - Increase awareness and preparedness
  - Adapt and implement (training and lessons learned)

4

THE SCENARIO

- Scenario locations and actors are **fictional**
- This is a **non-partisan** event
- State, county, and municipal characteristics are modeled after those found in our great **State of Wisconsin**

5

THE SCENARIO

- Every scenario is based on something that has happened, or been attempted (either in Wisconsin or elsewhere) - **these threats are real!**
- Just like real life, there will be times that you have **imperfect information** and must still make a decision

6

THE SCENARIO

- There will be media injects
- Press statements/releases may be necessary
- Think about your communications strategy and USE IT (your public statements <u>really</u> do matter!)

7

TTX AGENDA

- 15 mins — Tabletop Exercise Introduction (right now)
- 20 mins — Phase I Planning – Planning/Existing Security Measures
- 15 mins — Break
- 75+ mins — Phase II Scenario Overview;
  Election Day Tabletop Exercise (TTX)

  Timeline: 6:00 a.m. to 8:00 p.m. (?)

  Start at 6:00 a.m.; polls open from 7:00 a.m. – 8:00 p.m;
  polling place hours may be extended
- 30 mins — "Right Answers" Discussion / After Action Review (AAR)

8

WHY ARE WE HERE?

"The American public's confidence that their vote counts – and is counted correctly – relies on secure election infrastructure."

-Kirstjen Nielsen, Secretary of Homeland Security

(https//www.dhs.gov/topic/election-security)

9

Questions?

10

PRESENTED BY WISCONSIN ELECTIONS COMMISSION STAFF:

Michelle R. Hawley
Michelle.Hawley@wisconsin.gov
608-261-2004

Riley Willman
Riley.Willman@wisconsin.gov
608-261-2030

Tony Bridges (Election Security Lead)
Tony.Bridges@wisconsin.gov
608-266-0118

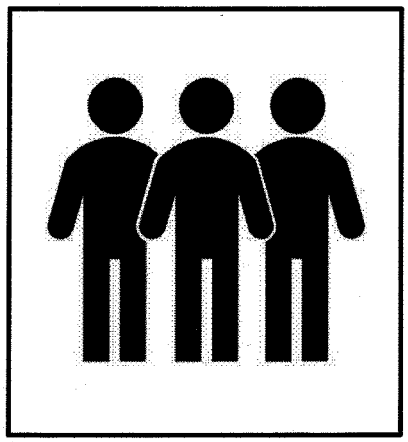
ELECTION SECURITY TRAINING AND TABLETOP EXERCISE (TTX) SCENARIO OVERVIEW

WISCONSIN ELECTIONS COMMISSION

JUNE 2018

1

POTENTIAL THREAT ACTORS



- Nation State Actors
- Politically Motivated Groups
- Hackers
- Terrorists
- Criminals
- Insiders

2

POTENTIAL THREAT MOTIVATIONS


FINANCIAL


FAME / REPUTATION


FOREIGN POLICY / INTERESTS


RETRIBUTION FOR PERCEIVED GRIEVANCES


SPREAD SOCIAL DIVISION


DESTABILIZE POLITICAL OPPOSITION


CHAOS / ANARCHY


UNDERMINE TRUST IN DEMOCRACY

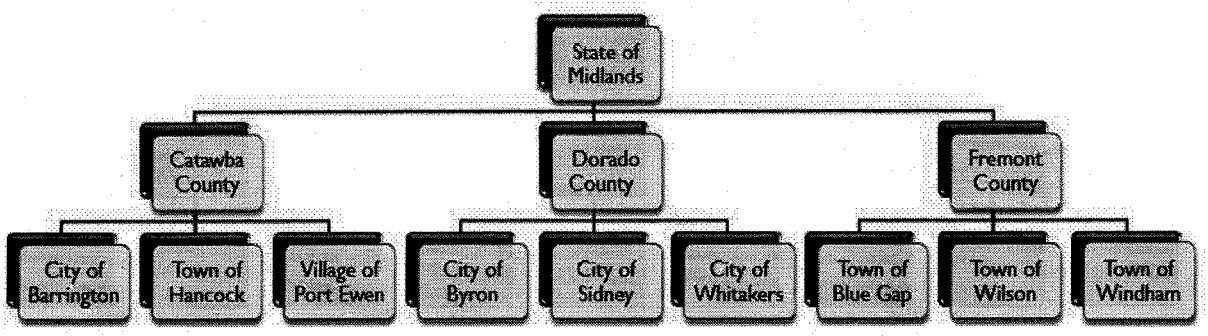
3

UPCOMING STATE ELECTION

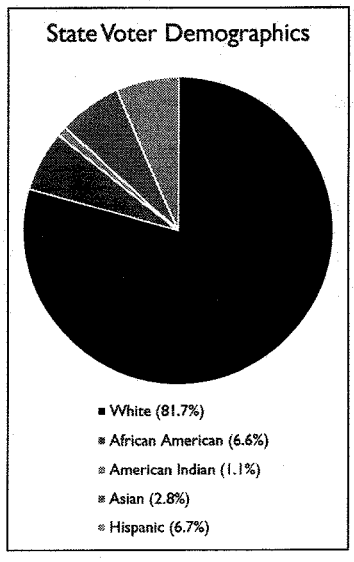
- First State election since suggestion of foreign meddling
- Media outlets focusing on election security
- Social media sites contain high election related content – extensive postings regarding upcoming elections and used as primary mode for information gathering and impression shaping by voters

4

THE STATE OF MIDLANDS



5

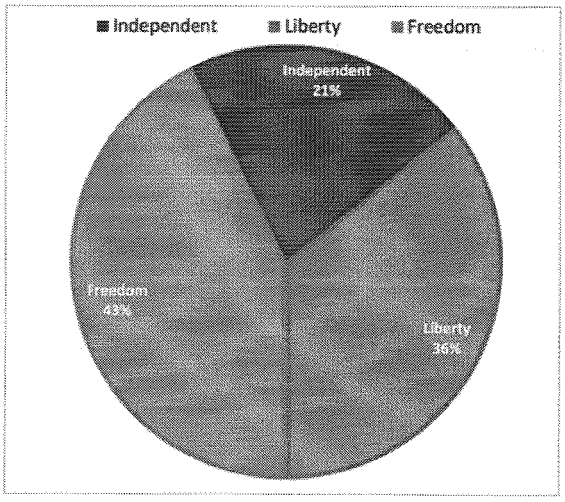


STATE OVERVIEW

- **Total population:** 5.8 million
- **Registered voters:** 3.1 million (Decentralized)
- **Voter Registration:** Online, by mail, or in person;
  same day voter registration;
  paper and electronic poll books
- **Voter Registration Database:** MidVote
- **Post Election Audit:** Voting Equipment only
- **Two Major Parties:** Liberty and Freedom
- **Voter Identification Requirements:** Voters must have valid photo identification

6

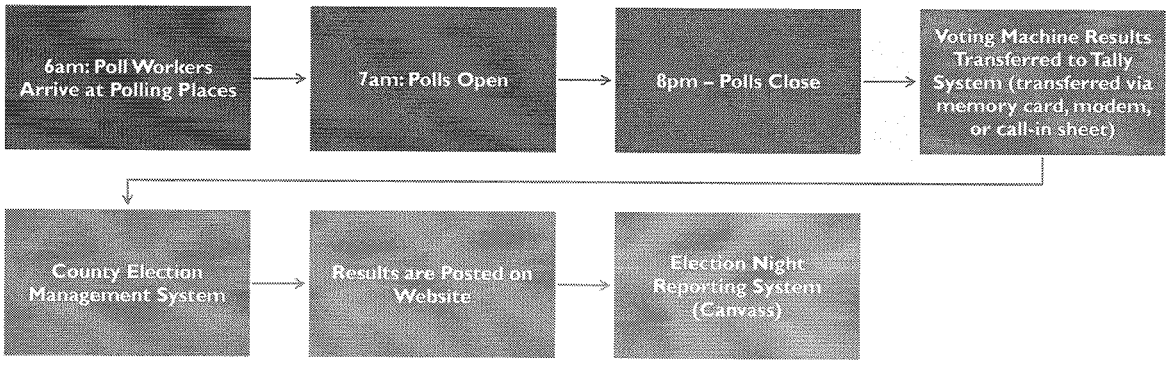
Registered Voters By Party



POLITICAL PARTIES

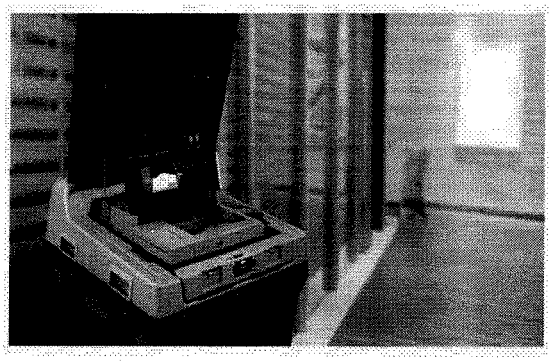
7

ELECTION DAY OPERATIONAL FLOW



8

VOTING MACHINES: CATAWBA AND DORADO COUNTIES



ES&S DS200 Optical Scanner

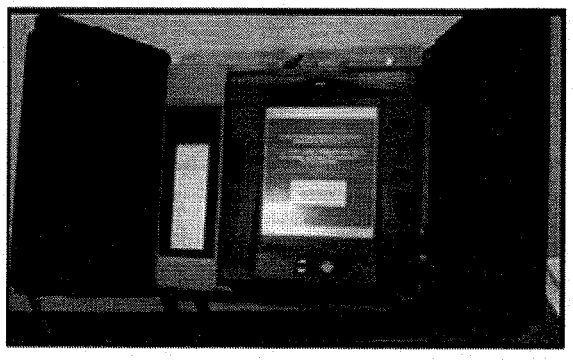
- Voter fills in paper ballot
- Paper ballot is scanned at optical scanner which confirms voter selection
- Paper ballot is then retained by polling site
- Results are uploaded by the municipality to the county via cellular signal

9

VOTING MACHINES: FREMONT COUNTY

ES&S iVotronic: Direct-Recording Electronic Voting Machine with VVPAT

- Voter makes selection on machine screen
- After selection, machine adds vote to internal machine total vote tally
- Voters sees vote submitted on screen and is NOT provided a print out
- Machine retains paper receipt of votes
- Vote tallies transferred via removable media at end of election day



10

ADDITIONAL INFORMATION

- We want you to have the most thought provoking, productive, and informative experience possible . . . we have intentionally omitted some scene details . . . go with it
- Scenario might be different than what happens in your county and/or municipalities – it is true to the TTX
- Most scenarios/injections require action/resolution (e.g. – contact another agency)
- You will be questioned by the media

11

ADDITIONAL INFORMATION

- Your actions don't count unless they are documented . . . be sure to write them on log (or directly on paper injects) we provided
- Resources
  - Each other / Moderators
  - Election Administration Manuals
  - Election Day Manuals
- Budget (not specifically addressed in this exercise) – keep in mind

12

REMEMBER YOUR PURPOSE

Protect Election Integrity

Preserve Public Trust

Defend Democracy!

13

Questions?

14