

After Action Report

Election Infrastructure Misinformation Reporting

2020 General Election

Aaron Wilson

Sr. Director, Election Security

Ben Spear

Director, Election Infrastructure Information Sharing
and Analysis Center (EI-ISAC)

Mike Garcia

Sr. Advisor, Election Security

February 2021

Contents

Summary	1
Misinformation in the Context of the 2020 Elections	3
The CIS Approach	4
Analysis of Outcomes	5
Volume over Time	5
Content over Time	5
Actions Resulting from Reported Cases	6
Identification of Cases by Source	6
Cases by Platform	6
Challenges and Recommendations	8
Uncontained Spread	8
Content Based Misinformation	9
Social Media Platform Engagement	9
Unmoderated Platforms	10
Early Detection and Analysis Partner	10
A Permanent Home	11
Misinformation Reporting Portal	12
Operational Efficiencies	12
Conclusions and Next Steps	13

Summary

The Center for Internet Security (CIS) worked with election officials and other stakeholders to facilitate election officials' ability to report misinformation related to election infrastructure during the 2020 general election. Stakeholders involved in development included the Cybersecurity and Infrastructure Security Agency (CISA), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).

The CIS election security team began developing plans and relationships related to misinformation reporting nearly a year prior to the 2020 general election. The primary goals were to:

- Provide state and local election officials with a single point of reporting for misinformation and disinformation across the major social media platforms to ease the burden of reporting on election offices.
- Collect the information necessary for social media platforms to investigate claims.
- Facilitate information sharing between election officials in different jurisdictions about what they are seeing, what to look out for, etc.
- Provide meaningful feedback to election officials on the status of their reports.

A misinformation reporting system was implemented for the 2020 general election to meet these goals. The reporting system flow allowed election officials to report a case of election infrastructure misinformation to a single source regardless of the platform(s) on which it appeared. The CIS election security team monitored this system 24x7 from September 28, 2020, through November 6, 2020, when it converted to a 12-hours a day, five days a week shift until mid-December.

CIS worked with the Election Integrity Partnership (EIP)¹ to provide additional information on individual reports and highlight emerging trends. EIP is a collection of social media research groups headed by the Internet Observatory at Stanford University. EIP provided additional analysis on misinformation reports from election officials and alerted CIS to emerging narratives that needed attention from election officials. In cases identified by EIP, CIS was able to alert election officials and address the misinformation jointly with the election official and EIP.

In total, CIS handled 209 misinformation cases—164 from election officials or their representatives and 45 from EIP—increasing through the election and then tapering off in the weeks following the election.

¹ The Election Integrity Partnership was created at Stanford University building on the partnership between the Stanford Internet Observatory and Program on Democracy and the Internet, Graphika, the Atlantic Council's Digital Forensic Research Lab, and the University of Washington's Center for an Informed Public.

Misinformation cases ranged from what appeared to be intentional disinformation to honest mistakes. CIS received several low-engagement cases (i.e., posts with few likes and shares) and platform-specific issues (e.g., auto-generated Facebook pages). CIS also saw several non-social media cases such as phone and text messaged-based misinformation as well as independent websites created to propagate misinformation. These were forwarded to appropriate authorities.

As we discuss later in this document, we received mixed results from the major social media platforms. For example, while CIS expected that social media platforms would act on any misinformation reported through CIS regardless of its reach on the respective platforms, we learned that Twitter was using some measure of “consequence” in its decision-making.

While there is room for improvement, we believe the reporting process was very successful for the 2020 general election and provided an important channel for election officials to address misinformation. Preliminary feedback from stakeholders suggests election officials found significant value in the process and, especially, having a central point for reporting misinformation. We provide more analysis and recommendations for next steps in the sections that follow.

Misinformation in the Context of the 2020 Elections

The 2016 election highlighted the risk to U.S. elections posed by two related threats:

- 1 Direct attacks on election infrastructure threatening to undermine the availability and integrity of elections or, as an alternative, undermine confidence in elections in the process
- 2 Information operations to influence public perception about the election process, candidates, and issues largely perpetrated by foreign actors

The rise in use of social media has reduced the level of effort necessary to reach large numbers of individuals, and removed the validation filters designed to prevent disinformation, such as publication standards for traditional media outlets. This led to a meteoric rise in misinformation in the 2016 election season, with information operations focused on shifting perceptions of candidates and public policy issues.²

In early 2018, the Election Infrastructure Subsector Government Coordinating Council established the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) to protect election technology systems and facilitate information sharing across the sector. The EI-ISAC is run by CIS through funding from CISA and in partnership with NASS, NASED, and election officials.

Through the 2018 election cycle, it became clear efforts to protect infrastructure were necessary but not alone sufficient for defending American democracy. In addition to using misinformation to influence matters of political and civil consequence, it became apparent misinformation could effectively be used to undermine confidence in elections even as the actual security of election infrastructure was increasing. Most misinformation activity in 2016 was the result of foreign actors generating and promoting disinformation. Analysis has shown, over the course of 2018, misinformation was increasingly driven by domestic users.³ As we approached 2020, we expected that both foreign and domestic misinformation could combine to create an even larger challenge than in previous election cycles.

As 2020 progressed, the risk of misinformation having an outsized impact on confidence in the election increased substantially with the election administration changes precipitated by the SARS-COV-2/COVID-19 pandemic. Typical election administration changes take years to implement and are accompanied by large public information campaigns to ensure voters understand the voting process. In contrast, the large-scale election administration changes made in response to the pandemic, and accompanying legal challenges, created a perfect scenario for mis- and disinformation to flourish.

² See, for instance, Allcott, Gentzkow, and Yu. "Trends in the diffusion of misinformation on social media." Research and Politics, April-June 2019. <https://journals.sagepub.com/doi/pdf/10.1177/2053168019848554>.

³ See, for instance, <https://www.washingtonpost.com/technology/2018/11/06/forget-russians-this-election-day-its-americans-peddling-disinformation-hate-speech/>.

The CIS Approach

As the 2020 election season approached, EI-ISAC member feedback indicated CIS could facilitate election officials' efforts to report misinformation about election infrastructure to social media platforms. Each social media company provides separate avenues for election officials to report misinformation. In some cases, these direct reporting options were only available to state election officials. The lack of a single reporting workflow led to confusion and inefficiency in reporting and responding to election misinformation. Through the support of a grant from the Democracy Fund, CIS began developing a web-based interactive platform, the Misinformation Reporting Portal (MiRP)⁴, as a means for facilitating interaction between election officials and their representatives, CISA, CIS, and social media platforms.

As the general election neared, concerns about onboarding election officials and platforms to a new portal led to the delay in deploying the MiRP until after the 2020 general election. As a replacement, CIS rolled out a simplified messaging approach to serve as the single reporting workflow.

When misinformation reports were received, CIS personnel reviewed the reports for completeness, verified the sender was an election official, and then processed reports from valid election officials. Each report was identified as a case. For most cases, processing reports involved sending the report to personnel with the CISA Countering Foreign Interference Task Force who forwarded it to the appropriate social media company. This process was adopted as CISA had previously established a protocol for submitting misinformation findings to the social media companies. CIS and CISA worked together to ensure the reports were sent to the social media platform within an hour of their receipt by CIS. CIS communicated updates back to the election official as updates were made to the case.

CIS made no effort to attribute misinformation to its creators or look for coordination among misinformation, including differentiating of misinformation from disinformation. CIS saw itself as part of "first responder" efforts to triage misinformation; given the time-sensitivity of the 2020 general election, CIS chose to leave investigative efforts to others.

⁴ The Misinformation Reporting Portal (MiRP) was tested in the summer of 2020 with a number of election offices at the state and local levels, but at no time was it connected to the social media companies. While the feedback was positive, election officials and social media companies expressed concerns about the potential difficulty of a wide deployment close to the general election. Ultimately, CIS decided to delay full deployment of the Misinformation Reporting Portal until after the 2020 general election.

Analysis of Outcomes

This section provides basic analysis of the misinformation cases handled by CIS.

Volume over Time

CIS handled a gradually increasing volume of misinformation cases approaching the election, then tapering off after the election. More than half of all cases came in a 10-day period before, during, and after the election, with 20% coming in the seven days before Election Day, 17% coming on Election Day, and another 15% coming the two days following the election.

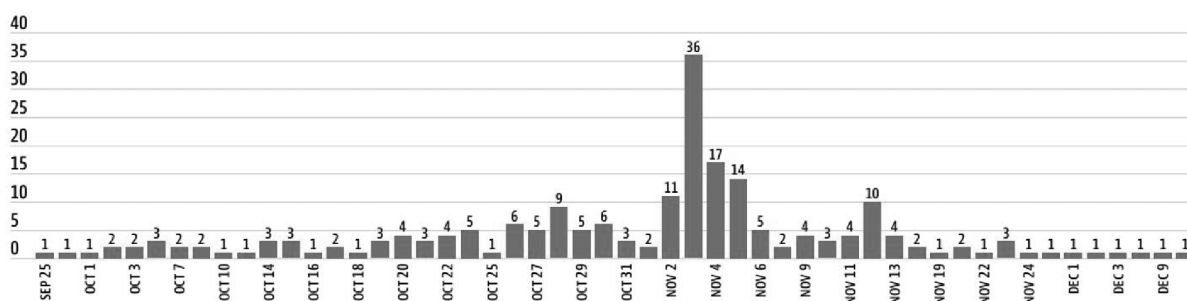


FIGURE 1. Raw number of Reports over Time

Content over Time

In addition to the expected increase in volume around the election, the content of misinformation changed over time. These narratives followed a predictable pattern based on the phase of the election. Specifically:

Pre-election	<ul style="list-style-type: none"> Public calls for voters to register that provided incorrect dates Claims of mail voting issues such as a voter claiming to have received multiple ballots or absentee ballots being destroyed in the mail
Election Day	<ul style="list-style-type: none"> Claims that typical election machine issues were nefarious and intended to sway the election Claims that typical election operations (e.g., movement of ballots) were improper and/or nefarious Association of election administration and other valid, practical changes (e.g., use of sharpies) with nefarious intentions Accounts claiming to have perpetrated fraud, such as by casting multiple ballots Claims of violations of campaigning laws (e.g., posting of campaign materials within restricted zones)
Election Night	<ul style="list-style-type: none"> Claims of ballot "stuffing" (i.e., electoral fraud where illegitimate ballots are added to the tally) Claims of intentional restriction of poll watchers Claims of manipulation of results by voting systems or super computers
Post-election	<ul style="list-style-type: none"> Claims of ballot stuffing continued Claims of results tampering by individuals and by machines Claims of suspicious foreign connections to voting system technology companies

Actions Resulting from Reported Cases

The misinformation reporting via CIS resulted in a positive action (i.e., content taken down or labeled) in 61% of cases. An additional 18% of cases achieved acceptable outcomes, including 8% that were reported only for awareness (i.e., no action was requested), and 10% were not related to social media (e.g., misinformation sent via text messages) and were handled by outside investigations such as law enforcement. Of the remaining 21%, 15% had no action by the relevant platform(s), 5% were collectively determined to not be misinformation, and 1% were rejected as coming from unverified senders.

Outcome	Count	Percentage
Awareness	18	8%
Inaction	32	15%
Not Misinformation	10	5%
Outside Investigation	20	10%
Acceptable Action	127	61%
Rejected	2	1%
Total	209	

Identification of Cases by Source

CIS handled cases from two primary sources: the EIP and election officials or their representatives. A question in our efforts was to determine if reporting through either of those sources was duplicative of each other or of efforts already being made by platforms.

In analysis of the reported cases, election officials tended to find misinformation that was specific to their organization or jurisdiction, likely based on parameters they had set themselves. The EIP found misinformation with increasing levels of engagement. This misinformation, as reported to CIS, did not overlap with misinformation reported by election officials.

Additionally, the misinformation cases reported to the platforms, whether directly or through the EIP, did not appear to overlap with what the social media platforms identified themselves. CIS believes that each of the three groups were focused on different things: officials on specific misinformation they could find in their own searches, the EIP on misinformation based on momentum, and social media platforms on identifiable campaigns and high-profile themes.

The lack of duplication suggests that, at minimum, all three efforts are necessary to identify—and combat—the full scope of misinformation.

Cases by Platform

Reports identified misinformation across 11 different media ‘channels.’ While originally designed for misinformation on social media platforms, CIS began receiving reports of misinformation on other media channels and attempted to address them. In addition to sharing all reports with CISA, some reports were shared with the Federal Bureau of Investigation and the Communications ISAC.

Misinformation reports on social media platforms weighed heavily toward Twitter, with nearly 62% of all cases. Facebook had the second highest volume, but was just 18% of cases. This is likely the result of the relative openness of Twitter, the pervasiveness of private groups on Facebook, and the favored approach of election officials and their staffs in reviewing content.

Platform	Count	Percentage
Citizen App	1	<1%
Email	6	3%
Facebook	37	18%
Facebook, Twitter	1	<1%
Google	1	<1%
Instagram	3	1%
Phone Calls	6	3%
Text Messaging	11	5%
TikTok	3	1%
Twitter	129	62%
Website	9	4%
YouTube	2	1%
Grand Total	209	

Challenges and Recommendations

In this section, we discuss the challenges faced during the 2020 election season, including the development of the MiRP and the challenges of operating the misinformation reporting email inbox. We also address recommended solutions to these challenges and potential enhancements of elections misinformation reporting in the future.

Uncontained Spread

We observed that certain activities made a given misinformation item or theme extremely difficult to contain. Most commonly, once the misinformation spread from its origin in social media and then to a news site – whether mainstream or alternative – it went from direct misinformation to reporting about misinformation. From that point, further amplification could be done by referring to the news report as “News organization X is reporting Y” which itself is not misinformation even though the content (the reported “Y”) is misinformation. We saw this trend used as a way to further amplify misinformation and skirt content-based policies of the social media companies.

This observation was accompanied by other related observations on the challenges and difficulties of social media companies to identify and address widespread misinformation.

- First, *we are not aware of any occasion where a social media company surfaced possible misinformation and brought it to our or an election official's attention.* From our assessment, the companies only responded to misinformation reports from us, the EIP, and election officials.
- Second, the level of action taken on identified misinformation was lacking in two ways: *posts were either labeled instead of removed*—this is especially true for the high engagement posts—and, second, the labels were often not appropriate to the content. It appeared as though labels were chosen for narrow pre-election issues and were not often updated to reflect the changing misinformation narratives through Election Day and afterwards.
- Third, there was seemingly *little effort from the social media companies to track down related or similar activity on their platform* based on what we reported.

Going into this project, we anticipated the social media companies had, or would use, far more sophisticated capabilities than what they demonstrated in reality. Based on discussions with the companies, we were led to believe that they were doing misinformation hunting themselves, and we expected they could take a report from an election official and perform broader analysis and action across their platform—for instance, by finding posts with matching text or images and flagging or removing those posts. We did not see either of these capabilities in action for election misinformation. It is possible that they were doing this but not as aggressively as we anticipated; or it is possible that they were doing this but the quantity of misinformation exceeded their ability to address it. This required CIS and its partners to continue to track and identify related activity to send to the social media platforms for action.

Content Based Misinformation

We noticed that the mechanism required to determine mis- and disinformation for this election was almost entirely a content-based operation, as opposed to account-based operations. Account based operations look for coordinated inauthentic behavior from an account or collection of accounts working together. This has been seen in many influence operations perpetrated by foreign actors. However, our cases were not clearly linked to a pattern of inauthentic behavior but, instead, had to be handled based on the content of the post itself (i.e., we had to determine if the content itself was incorrect). This required three criteria for action:

- Verify the content is incorrect
- Provide proof to the social media company that the content is incorrect
- Satisfactorily demonstrate to the social media company that the incorrect information has sufficient consequence to warrant their action

In some cases, these three criteria were easy to meet and others more challenging. We often received cases directly from election officials who are the authority on whether the information was correct (meeting criterion #1), and in those cases the authoritativeness of the election official was sufficient to meet criterion #2. In most of these cases, the social media companies acted without additional justification (criterion #3).

The harder cases, however, were the ones CIS had to work with election officials to obtain the ground truth, and then present it to the social media companies. These cases were often more consequential and important, primarily because cases identified by the EIP typically had or were gaining traction quickly on the platforms. Developing a model that can more quickly move through these three steps is essential for future handling of election infrastructure misinformation.

Social Media Platform Engagement

Over time we observed different levels of engagement from the social media platforms, notably Twitter and Facebook. We first engaged both platforms about the Misinformation Reporting Portal in early 2020 and held a series of meetings to discuss the concept of automated exchange of data. Both platforms raised concerns. Facebook never agreed to participate. Twitter was willing to participate at one point; however, a security incident at Twitter in July 2020 forced them to reevaluate and cease their involvement for 2020.

When we determined with CISA, NASED, and NASS to move forward with an email-based approach, we did not request permission; reactions from the platforms were mixed. We did not receive any pushback from Twitter. However, Facebook advised election officials to report directly to Facebook instead of through CIS. Nevertheless, throughout the election cycle, both Twitter and Facebook engaged with the reporting workflow and serviced election officials' cases reported through the EI-ISAC. We did not always agree with the level of action they took on individual cases, but their engagement was notable.

As we move forward, it will be critical to define the roles of all involved parties and for those entities, especially the social media platforms, to accept their role. Specifically, Facebook has strongly positioned themselves to engage directly with election officials to the exclusion of third parties. While this has some benefits in specific Facebook-only cases, it is not the best approach to deal with election infrastructure misinformation as a broader issue, nor is it the most effective approach for election officials themselves. Addressing the broader issue will involve more transparency and cooperation from Facebook and other social media companies. There is currently no leverage to compel them to do so.

Unmoderated Platforms

As the election cycle progressed, we noticed the use of unmoderated platforms such as 4chan, 8kun, Gab, and Parler. This underscores a concerning trend in our efforts to mitigate election infrastructure misinformation: even if we improve the ability to detect and mitigate activity on mainstream social media platforms such as Twitter and Facebook, users may opt to continue this activity on less moderated platforms. Any future regulatory efforts to support combating misinformation must ensure that all current and future social media platforms are held to the same standard.

Early Detection and Analysis Partner

The Election Integrity Partnership (EIP) provided significant assistance to the project. The most important and consequential cases were often surfaced by the EIP, run to ground by CIS with the relevant election officials, and then reported to the relevant social media company. This model of early detection of possible misinformation, quick sourcing of the truth, and action from the platform is the primary workflow to repeat and scale in future efforts. This model would also be significantly improved if the social media companies were detecting possible misinformation and reporting it to CIS for sourcing the truth from election officials.

Examples:

- **Ballots Stolen Misinformation**

On Election Day, the EIP reported a series of posts gaining momentum that included a video of an individual purportedly moving a large ballot box into a parked vehicle. The text of these posts varied, but generally raised questions as to whether these ballots were being stolen.

After receiving news of these posts from the EIP, CIS reached out to the election officials with the post. Within 10 minutes, an election official replied stating, "Authorized individual confirmed. I have ballots from him in my possession." CIS passed this information to Twitter through CISA, and the posts were labeled about 45 minutes later.

While CIS would have preferred Twitter remove the post, this example underscores the effectiveness of election officials' ability to provide ground truth on election administration matters.

- **Unauthorized Behavior Misinformation**

In early December, a video emerged on Twitter purportedly showing a voting system vendor employee inserting a USB drive into a ballot scanner. The EIP identified posts including this video and shared them with CIS.

CIS contacted county election officials, who informed CIS that the individual was a voting system technician moving a report from the server to the USB drive and then to a laptop for analysis. County officials indicated that this is necessary because the servers are locked down and have only the minimum necessary software.

CIS passed this information on to Twitter through CISA, and, within three hours, Twitter labeled the tweet and took “steps to limit trending.” The account that originated the misinformation was later suspended. This is an excellent example where only the election official could provide confirmation that the activities performed by the technician were not nefarious.

- **Machines Tampering Misinformation**

On Election Day, the EIP reported trending posts claiming that voting machine malfunctions in a large city were part of a larger campaign by a political party to disenfranchise voters. CIS communicated with the state election officials and confirmed the machine issues were typical malfunctions only affecting a small percentage of machines. This information was communicated to Twitter via the EIP within an hour of its initial report to CIS. Twitter subsequently removed the activity on their platform.

The EIP was a temporary organization of four research groups: Stanford Internet Observatory, Graphika, DFRLab, and University of Washington Center for Informed Public.⁵ Their efforts focused on early detection of viral misinformation and cross-platform analysis. A persistent and scalable version of this capability is critical to the future of handling election misinformation.

A Permanent Home

Misinformation will continue to impact elections and voter confidence in the years to come, and will likely become more complicated to address. With a proliferation of social media platforms and other communication channels, election officials have a continued need for assistance in reporting misinformation about their election infrastructure and processes.

After discussion with numerous stakeholders, CIS believes it is the natural home for this role. To this point, however, most misinformation work within CIS has occurred in the best practices side of the organization via grant funding from the Democracy Fund. As the program matures, ongoing operation should transition to the operational side of CIS, specifically within the EI-ISAC under CISA funding, likely requiring changes to the agreement between CISA and CIS.

⁵ <https://www.eipartnership.net/>

Misinformation Reporting Portal

Early CIS efforts focused on the development of the misinformation reporting portal and securing the buy-in from stakeholders necessary for the portal to be successful. This included election officials, their representatives at NASS and NASED, CISA, Twitter, and Facebook. CIS developed a prototype of the portal to demonstrate its potential and continued development through a round of operational testing with election officials and/or their communications staff from five states. The officials were particularly enthusiastic about the ability to see misinformation reports from other election offices. The portal interface was well received by election officials and updates were made based on their feedback to produce an initial production-ready version of the Misinformation Reporting Portal.

The portal, however, did not receive the support from Twitter and Facebook necessary to facilitate a seamless exchange of information with them on behalf of election officials. Various reasons were given by Twitter and Facebook representatives for their lack of support. The most prominent reason was a lack of time to negotiate an information exchange protocol. CIS offered to accommodate any method and format the platform desired for submitting reports and receiving feedback, but their opposition to the portal remained.

An additional concern involved onboarding election officials onto the portal and training them for use. For this election, the biggest issue was timing; the portal was not ready for widescale adoption until late summer, leaving little time to train and resolve problems. With the pressure of the 2020 election lifted, more time can be taken for a coordinated rollout. CIS is also developing an elections misinformation dashboard for members that will expand the use of the portal from being primarily a misinformation reporting tool to providing the ability to rapidly see the broader misinformation landscape as reported to CIS. In addition, CIS is looking to integrate its misinformation reporting tool into a multi-function EI-ISAC portal that will streamline the process of reporting. Nonetheless, some officials are likely to prefer alternate submission processes, and CIS expects to continue the approach used in 2020 for the foreseeable future.

Operational Efficiencies

We noted operational areas that can be improved in future efforts. We summarize a couple of those here.

- **Expectation setting:** As we entered this effort, all parties lacked a full understanding of what to expect in terms of timing and outcomes. This led to some expectation gaps with election officials, which can be corrected in the future based on this experience.
- **Handling variety:** As mentioned, the reporting workflow was set up to handle social media-based misinformation, but received other reports related to misinformation. The unexpected cases were handled slower than others and with more inconsistency. Developing the necessary relationships and procedures for this variety of cases and channels is critical to future efforts. Homing the efforts inside the EI-ISAC permanently will assist with this.

Conclusions and Next Steps

This election infrastructure reporting workflow for the 2020 general election improved the reporting process for election infrastructure mis- and disinformation, and identified a clear path forward for future elections. To ensure continued attention on these issues, the capabilities demonstrated by CIS should be moved formally into the scope of the EI-ISAC.








The EI-ISAC can leverage its current capabilities and relationships to continue the effort to build the misinformation reporting portal and strengthen the relationships with stakeholders and the social media companies. This is an ever-changing problem and developing strong relationships with clear roles for each party, and technology solutions to support those roles, is the best approach to adapting and scaling to address the problem. Maturing the capabilities, we demonstrated through the 2020 general election—identification of possible misinformation, sourcing of truth, and taking action—in the years to come will take a significant effort from many organizations. CIS looks forward to playing a substantial role in that important journey.

These efforts to support election officials in 2020 were successful, and we are proud of the work accomplished on their behalf and with their help. We see a better and more secure future when we can fully operationalize our efforts and follow the suggestions presented in this report.

CIS would like to extend a special thanks to the state and local election officials who participated, as well as staff from the National Association of State Election Directors (NASED), National Association of Secretaries of State (NASS), and Cybersecurity and Infrastructure Security Agency (CISA) for their efforts throughout the project.



The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

 www.cisecurity.org
 info@cisecurity.org
 518-266-3460
 Center for Internet Security
 @CISecurity
 CenterforIntSec
 TheCISecurity
 cisecurity