

From: [REDACTED]
Subject: Findings_Draft. PRE-DECISIONAL
Date: December 16, 2020 at 5:14 PM
To: bernardkerik [REDACTED]

kriess [REDACTED] genflynn [REDACTED]

Per conversation. This is the final draft document. For discussion and coordination

PRE-DECISIONAL

Sent from ProtonMail mobile



Findings_Draft.d
OCX

December 16, 2020

PRESIDENTIAL FINDINGS
TO PRESERVE COLLECT AND ANALYZE NATIONAL SECURITY INFORMATION
REGARDING THE 2020 GENERAL ELECTION

By the authority vested in me as President of the United States pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333, 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code:

I, Donald J. Trump, President of the United States, find that the forensic report of the Antrim County, Michigan voting machines, released December 13, 2020, and other evidence submitted to me in support of this order, provide probable cause sufficient to require action under the authorities cited above because of evidence of international and foreign interference in the November 3, 2020, election. Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests. The forensic report prepared by experts found that "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors... The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud." The report found the election management system to be wrought with unacceptable and unlawful vulnerabilities—including access to the internet—probable cause to find evidence of fraud, and numerous malicious actions.

There is also probable cause to find that Dominion Voting Systems, Smartmatic, Electronic Systems & Software, and Hart Inter.Civic, Clarity Election Night Reporting, Edison Research, Sequoia, Scytl, and similar or related entities, agents or assigns, have the same flaws and were subject to foreign interference in the 2020 election in the United States. There is probable cause to find these systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in our election, in which there is probable cause to find votes were in fact altered and manipulated contrary to the will of the voters.

Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom. The Dominion Voting system is owned and controlled by foreign entities. Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks. In fact, there is probable cause to find a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017)

Just days prior to the election of November 3, 2020, federal Judge Totenberg found, after three days of testimony including by Dominion executive Eric Coomers:

There are “true risks posed by the new BMD [Ballot Marking Device of Georgia’s Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants’ and Dominion’s stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens’ confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems’ capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process.

“The Plaintiffs’ national cybersecurity experts convincingly present evidence that this is not a question of “might this actually ever happen?” – but “when it will happen,” especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, “we have never seen it,” the future does not bode well.

“Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State’s doorstep. The Court certainly hopes not.”¹

And, yet it did. Every defect and hazard of which Judge Totenberg warned happened in Georgia. Witnesses in Georgia have provided evidence of crashes, the replacement of a server, impermissible updates to the system, connections to the internet, and both Coffee and Ware counties have identified a significant percentage of votes being wrongly allocated contrary to the will of the voter. Coffee County Georgia has refused to certify its result.

Accordingly, I hereby order:

(1) Effective immediately, the Secretary of Defense shall seize, collect, retain and analyze all machines, equipment, electronically stored information, and material records required for retention under United States Code Title 42, Sections 1974-1974(e), including but not limited to those identified in footnote 1. The Secretary of Defense has discretion to determine the

¹ Case 1:17-cv-02989-AT Document 964 Filed 10/11/20 Page 146 of 147

interdiction of national critical infrastructure supporting federal elections. Designated locations will be identified in the operation order.

(2) Within 7 days of commencement of operations, the initial assessment must be provided to the Office of the Director of National Intelligence. The final assessment must be provided to the Office of the Director of National Intelligence no later than 60 days from commencement of operations.

(3) The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

(4) A direct liaison to be authorized to coordinate as required between the applicable U.S. Departments and Agencies.

(5) The Secretary of Defense may select by name or by unit federalization of appropriate National Guard support.

(6) The Assistant Secretary of Defense for Homeland Security will coordinate support requirements as needed from the Department of Homeland Security.

(7) The appointment of a Special Prosecutor to oversee this operation and institute all criminal and civil proceedings as appropriate based on the evidence collected and provided all resources necessary to carry out her duties consistent with federal laws and the Constitution.

From: GenFlynn [REDACTED]
Subject: Re: Findings_Draft. PRE-DECISIONAL



Date: December 16, 2020 at 5:50 PM

To: [REDACTED] bernardkerik [REDACTED] kfriess [REDACTED]

I reviewed. Fix the spelling error in the title. Ensure it gets a legal review, but this is ready to go from my standpoint. Thanks for getting the key points in.

FLYNN

Sent from ProtonMail Mobile

On Wed, Dec 16, 2020 at 4:14 PM, [REDACTED] wrote:

Per conversation. This is the final draft document. For discussion and coordination

PRE-DECISIONAL

Sent from ProtonMail mobile

From: p [REDACTED]
Subject: Fw: Finding Docs
Date: December 17, 2020 at 8:46 AM
To: bernardkerik [REDACTED]

kfriess [REDACTED]

Final draft finding - includes DHS switch language as well as Foreign interference expansion and warrant issuance language.

PW

Sent from ProtonMail mobile

----- Original Message -----

On Dec 17, 2020, 8:44 AM, Russell Ramsland [REDACTED] wrote:

Empty message

publickey -

[REDACTED].asc

Findings
FINAL.docx

Foreign Election
Interfer...v1.pdf

December 17, 2020

PRESIDENTIAL FINDINGS
TO SEIZE, COLLECT, PRESERVE AND ANALYZE NATIONAL SECURITY
INFORMATION REGARDING THE 2020 GENERAL ELECTION

By the authority vested in me as President of the United States pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333, 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and Section 301 of Title 3, United States Code:

I, Donald J. Trump, President of the United States, find that the forensic report of the Antrim County, Michigan voting machines, released December 13, 2020, and other evidence and sworn testimony submitted to me in support of this order, provide probable cause sufficient to require action under the authorities cited above because of evidence of foreign interference and widespread fraud leading up to and including the November 3, 2020 election. Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests. The forensic report prepared by experts found that "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors... The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud." The report found the election management system to be wrought with unacceptable and unlawful vulnerabilities—including access to the internet—probable cause to find evidence of fraud, and numerous malicious actions.

There is also probable cause to find that Dominion Voting Systems, Smartmatic, Electronic Systems & Software, and Hart Inter Civic, Clarity Election Night Reporting, Edison Research, Sequoia, Scytl, Election Source and similar or related entities, agents or assigns, have the same flaws and were subject and vulnerable to foreign interference in the 2020 election in the United States. There is probable cause to find these systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in our election, in which there is probable cause to find votes were in fact altered and manipulated contrary to the will of the voters.

Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom. The Dominion Voting system is owned and controlled by foreign entities. Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks. In fact, there is probable cause to find a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017).

Just days prior to the election of November 3, 2020, federal Judge Totenberg found, after three days of testimony including by Dominion executive Eric Coomers:

There are “true risks posed by the new BMD [Ballot Marking Device of Georgia’s Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants’ and Dominion’s stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens’ confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems’ capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process.

“The Plaintiffs’ national cybersecurity experts convincingly present evidence that this is not a question of “might this actually ever happen?” – but “when it will happen,” especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, “we have never seen it,” the future does not bode well.

“Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State’s doorstep. The Court certainly hopes not.”¹

And, yet it did. Every defect and hazard of which Judge Totenberg warned happened in Georgia. Witnesses in Georgia have provided evidence of crashes, the replacement of a server, impermissible updates to the system, connections to the internet, and both Coffee and Ware counties have identified a significant percentage of votes being wrongly allocated contrary to the will of the voter. Coffee County Georgia has refused to certify its result.

Further foreign intelligence service involvement in the 2020 elections is evidenced by the involvement of Kavtech, a Pakistan based Business Intelligence firm with ties to the ISI (Pakistani Inter-Service Intelligence Agency), that directly received e-mails from the Nevada Secretary of State containing personally identifiable voter registration information. It is unknown how this information may have been exploited. (see attachment).

¹ Case 1:17-cv-02989-AT Document 964 Filed 10/11/20 Page 146 of 147

Accordingly, I hereby order:

- (1) Effective immediately, the Secretary of Homeland Security shall seize, collect, preserve, protect, retain and analyze all machines, equipment, electronically stored information, and material records required for retention under United States Code Title 42, Sections 1974-1974(e), including but not limited to those identified in footnote 1. The Secretary of Homeland Security has discretion to determine the interdiction of federal and state critical infrastructure that supported the federal elections of 2020, including hardware, software, documentation, ballots, key cards and any other physical items to include security badges, polling official rosters, and related items. Designated locations will be identified in the operation order.
- (2) The Secretary of Homeland Security and all of the Secretary's agents and assigns shall have the power to immediately seek the issuance of any and all search warrants and other warrants or legal powers as may be necessary to carry out and execute this directive.
- (3) Within 7 days of commencement of operations, the initial assessment of information and physical items seized in the above order must be provided to the Office of the Director of National Intelligence. The final assessment must be provided to the Office of the Director of National Intelligence no later than 60 days from commencement of operations.
- (4) In accordance with my Executive Order dated September 2018, the Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense and the Attorney General.
- (5) A direct liaison is authorized to coordinate as required between the applicable U.S. Departments and Agencies. Director, National Intelligence shall ensure access to classified information is made available to those with appropriate clearances. Director, National Intelligence is authorized to provide additional compartmented "read on" where applicable. These special category indoctrinations will be limited in scope with focus on foreign influence in national elections.
- (6) The Secretary of Homeland Security shall request the Secretary of Defense to provide select personnel/capabilities by name or by unit (federalization of appropriate National Guard assets authorized) in support of a Defense Support to Civil Authorities (DSCA) mission.
- (7) The Assistant Secretary of Defense for Homeland Security shall coordinate support requirements as needed from the Department of Defense.
- (8) The appointment of a Special Prosecutor to oversee this operation and institute all criminal and civil proceedings as appropriate based on the evidence collected and provided all resources necessary to carry out her duties consistent with federal laws and the Constitution.