Table of Contents

Alert (AA20-304A)

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

Original release date: October 30, 2020 | Last revised: November 03, 2020

Summary

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020. [1] (Reference FBI FLASH message ME-000138-TT, disseminated October 29, 2020). Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election.

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8 framework. See the ATT&CK for Enterprise version 8 for all referenced threat actor techniques.

Click here for a PDF version of this report.

1. This disinformation (hereinafter, "the propaganda video") was in the form of a video purporting to misattribute the activity to a U.S. domestic actor and implies that individuals could cast fraudulent ballots, even from overseas. https://www.odni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

Technical Details

Analysis by CISA and the FBI indicates this actor scanned state websites, to include state election websites, between September 20 and September 28, 2020, with the Acunetix vulnerability scanner (*Active Scanning: Vulnerability Scanning* [T1595.002]). Acunetix is a widely used and legitimate web scanner, which has been used by threat actors for nefarious

purposes. Organizations that do not regularly use Acunetix should monitor their logs for any activity from the program that originates from IP addresses provided in this advisory and consider it malicious reconnaissance behavior.

Additionally, CISA and the FBI observed this actor attempting to exploit websites to obtain copies of voter registration data between September 29 and October 17, 2020 (*Exploit Public-Facing Application* [T1190]). This includes attempted exploitation of known vulnerabilities, directory traversal, Structured Query Language (SQL) injection, web shell uploads, and leveraging unique flaws in websites.

CISA and the FBI can confirm that the actor successfully obtained voter registration data in at least one state. The access of voter registration data appeared to involve the abuse of website misconfigurations and a scripted process using the cURL tool to iterate through voter records. A review of the records that were copied and obtained reveals the information was used in the propaganda video.

CISA and FBI analysis of identified activity against state websites, including state election websites, referenced in this product cannot all be fully attributed to this Iranian APT actor. FBI analysis of the Iranian APT actor's activity has identified targeting of U.S. elections' infrastructure (*Compromise Infrastructure* [T1584]) within a similar timeframe, use of IP addresses and IP ranges—including numerous virtual private network (VPN) service exit nodes—which correlate to this Iran APT actor (*Gather Victim Host Information* [T1592)]), and other investigative information.

Reconnaissance

The FBI has information indicating this Iran-based actor attempted to access PDF documents from state voter sites using advanced open-source queries (*Search Open Websites and Domains* [T1593]). The actor demonstrated interest in PDFs hosted on URLs with the words "vote" or "voter" and "registration." The FBI identified queries of URLs for election-related sites.

The FBI also has information indicating the actor researched the following information in a suspected attempt to further their efforts to survey and exploit state election websites.

- YOURLS exploit
- Bypassing ModSecurity Web Application Firewall
- Detecting Web Application Firewalls
- SQLmap tool

Acunetix Scanning

CISA's analysis identified the scanning of multiple entities by the Acunetix Web Vulnerability scanning platform between September 20 and September 28, 2020 (*Active Scanning: Vulnerability Scanning* [T1595.002]).

The actor used the scanner to attempt SQL injection into various fields in `/registration` `/registration/details` with status codes 404 or 500.

TLP:WHITE

```
/registration/registration/details?addresscity=-1 or
3*2<(0+5+513-513) -- &addressstreet1=xxxxx&btnbeginregistration=begin
voter registration&btnnextelectionworkerinfo=next&
btnnextpersonalinfo=next&btnnextresdetails=next&
btnnextvoterinformation=next&btnsubmit=submit&chkageverno=on&
chkageveryes=on&chkcitizenno=on&chkcitizenyes=on&chkdisabledvoter=on&
chkelectionworker=on&chkresprivate=1&chkstatecancel=on&dlnumber=1&
dob=xxxx/x/x&email=sample@email.tst&firstname=xxxxx&gender=radio&
hdnaddresscity=&hdngender=&last4ssn=xxxxx&lastname=xxxxxinjjeuee&
mailaddresscountry=sample@xxx.xxx&mailaddressline1=sample@email.tst&
mailaddressline2=sample@xxx.xxx&mailaddressline3=sample@xxx.xxx&
mailaddressstate=aa&mailaddresszip=sample@xxxx.xxx&
mailaddresszipex=sample@xxx.xxx&middlename=xxxxx&overseas=1&
partycode=a&phoneno1=xxx-xxx-xxxx&phoneno2=xxx-xxx-xxxx&radio=consent&
statecancelcity=xxxxxxx&statecancelcountry=usa&statecancelstate=XXaa&
statecancelzip=xxxxx&statecancelzipext=xxxxx&suffixname=esq&
txtmailaddresscity=sample@xxx.xxx
```

Requests

The actor used the following requests associated with this scanning activity.

```
2020-09-26 13:12:56 x.x.x.x GET /x/x v[$acunetix]=1 443 - x.x.x.x
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+
(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 200 0 0 0

2020-09-26 13:13:19 X.X.x.x GET /x/x voterid[$acunetix]=1 443 -
x.x.x.x Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+
(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 200 0 0 1375

2020-09-26 13:13:18 .X.x.x GET /x/x voterid=;
print(md5(acunetix_wvs_security_test)); 443 - X.X.x.x
```

User Agents Observed

CISA and FBI have observed the following user agents associated with this scanning activity.

```
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+
(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 500 0 0 0

Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-US;+rv:1.9b4)+Gecko
/2008031318+Firefox/3.0b4

Mozilla/5.0+(X11;+U;+Linux+i686;+en-US;+rv:1.8.1.17)+Gecko
/20080922+Ubuntu/7.10+(gutsy)+Firefox/2.0.0.17
```

Exfiltration

Obtaining Voter Registration Data

TLP:WHITE

Following the review of web server access logs, CISA analysts, in coordination with the FBI, found instances of the cURL and FDM User Agents sending GET requests to a web resource associated with voter registration data. The activity occurred between September 29 and October 17, 2020. Suspected scripted activity submitted several hundred thousand queries iterating through voter identification values, and retrieving results with varying levels of success [*Gather Victim Identity Information* (T1589)]. A sample of the records identified by the FBI reveals they match information in the aforementioned propaganda video.

Requests

The actor used the following requests.

```
2020-10-17 13:07:51 x.x.x.x GET /x/x voterid=XXXX1 443 - x.x.x.x
curl/7.55.1 - 200 0 0 1406

2020-10-17 13:07:55 x.x.x.x GET /x/x voterid=XXXX2 443 - x.x.x.x
curl/7.55.1 - 200 0 0 1390

2020-10-17 13:07:58 x.x.x.x GET /x/x voterid=XXXX3 443 - x.x.x.x
curl/7.55.1 - 200 0 0 1625

2020-10-17 13:08:00 x.x.x.x GET /x/x voterid=XXXX4 443 - x.x.x.x
curl/7.55.1 - 200 0 0 1390
```

Note: incrementing `voterid` values in `cs_uri_query` field

User Agents

CISA and FBI have observed the following user agents.

```
FDM+3.x

curl/7.55.1

Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+
(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 500 0 0 0
Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-US;+rv:1.9b4)+Gecko
/2008031318+Firefox/3.0b4
```

See figure 1 below for a timeline of the actor's malicious activity.

TECHNICAL FINDINGS

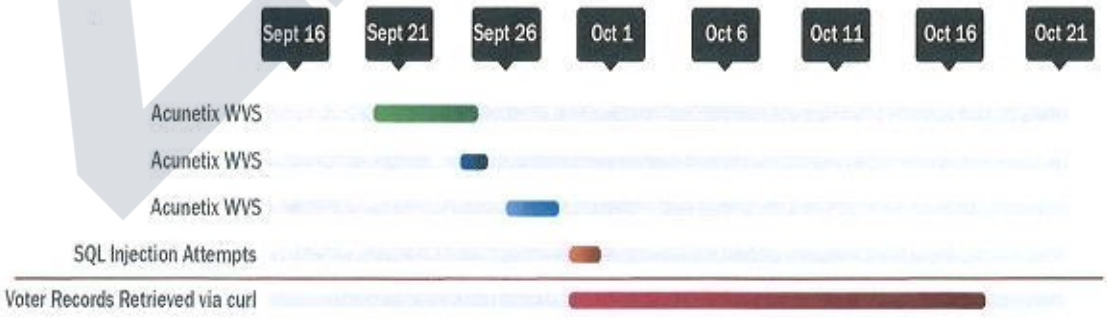


Figure 1: Overview of malicious activity

TLP:WHITE

Mitigations

Detection

Acunetix Scanning

Organizations can identify Acunetix scanning activity by using the following keywords while performing log analysis.

- `$acunetix`
- `acunetix_wvs_security_test`

Indicators of Compromise

For a downloadable copy of IOCs, see AA20-304A.stix.

Disclaimer: *many of the IP addresses included below likely correspond to publicly available VPN services, which can be used by individuals all over the world. This creates the potential for a significant number of false positives; only activity listed in this advisory warrants further investigation. The actor likely uses various IP addresses and VPN services.*

The following IPs have been associated with this activity.

- 102.129.239[.]185 (Acunetix Scanning)
- 143.244.38[.]60 (Acunetix Scanning and cURL requests)
- 45.139.49[.]228 (Acunetix Scanning)
- 156.146.54[.]90 (Acunetix Scanning)
- 109.202.111[.]236 (cURL requests)
- 185.77.248[.]17 (cURL requests)
- 217.138.211[.]249 (cURL requests)
- 217.146.82[.]207 (cURL requests)
- 37.235.103[.]85 (cURL requests)
- 37.235.98[.]64 (cURL requests)
- 70.32.5[.]96 (cURL requests)
- 70.32.6[.]20 (cURL requests)
- 70.32.6[.]8 (cURL requests)
- 70.32.6[.]97 (cURL requests)
- 70.32.6[.]98 (cURL requests)
- 77.243.191[.]21 (cURL requests and FDM+3.x [Free Download Manager v3] enumeration/iteration)
- 92.223.89[.]73 (cURL requests)

CISA and the FBI are aware the following IOCs have been used by this Iran-based actor. These IP addresses facilitated the mass dissemination of voter intimidation email messages on October 20, 2020.

- 195.181.170[.]244 (Observed September 30 and October 20, 2020)

TLP:WHITE

- 102.129.239[.]185 (Observed September 30, 2020)
- 104.206.13[.]27 (Observed September 30, 2020)
- 154.16.93[.]125 (Observed September 30, 2020)
- 185.191.207[.]169 (Observed September 30, 2020)
- 185.191.207[.]52 (Observed September 30, 2020)
- 194.127.172[.]98 (Observed September 30, 2020)
- 194.35.233[.]83 (Observed September 30, 2020)
- 198.147.23[.]147 (Observed September 30, 2020)
- 198.16.66[.]139(Observed September 30, 2020)
- 212.102.45[.]3 (Observed September 30, 2020)
- 212.102.45[.]58 (Observed September 30, 2020)
- 31.168.98[.]73 (Observed September 30, 2020)
- 37.120.204[.]156 (Observed September 30, 2020)
- 5.160.253[.]50 (Observed September 30, 2020)
- 5.253.204[.]74 (Observed September 30, 2020)
- 64.44.81[.]68 (Observed September 30, 2020)
- 84.17.45[.]218 (Observed September 30, 2020)
- 89.187.182[.]106 (Observed September 30, 2020)
- 89.187.182[.]111 (Observed September 30, 2020)
- 89.34.98[.]114 (Observed September 30, 2020)
- 89.44.201[.]211 (Observed September 30, 2020)

Recommendations

The following list provides recommended self-protection mitigation strategies against cyber techniques used by advanced persistent threat actors:

- Validate input as a method of sanitizing untrusted input submitted by web application users. Validating input can significantly reduce the probability of successful exploitation by providing protection against security flaws in web applications. The types of attacks possibly prevented include SQL injection, Cross Site Scripting (XSS), and command injection.
- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable unnecessary services and install available patches for the services in use. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP, and avoid using open RDP ports, unless there is a valid need. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- Apply multi-factor authentication, when possible.
- Maintain a good information back-up strategy by routinely backing up all critical data and system configuration information on a separate device. Store the backups offline, verify their integrity, and verify the restoration process.

- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access follow internal remote access policies.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as a VPNs. However, recognize the security of VPNs matches the security of the connected devices.
- Use security features provided by social media platforms; use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches and automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed of threat actors to create new exploits following the release of a patch. These "N-day" exploits can be as damaging as zero-day exploits. Ensure the authenticity and integrity of vendor updates by using signed updates delivered over protected links. Without the rapid and thorough application of patches, threat actors can operate inside a defender's patch cycle. [2] Additionally, use tools (e.g., the OWASP Dependency-Check Project tool [3]) to identify the publicly known vulnerabilities in third-party libraries depended upon by the application.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (e.g., SQL injection, cross-site scripting) by using a commercial web application vulnerability scanner in combination with a source code scanner. [4] Fixing or patching vulnerabilities after they are identified is especially crucial for networks hosting older web applications. As sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

Deploy a web application firewall (WAF) to prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware. [5] Malicious

cyber actors often deploy web shells—software that can enable remote administration—on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, remote access, or used on high-value assets. [6] Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs). [7] Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remediate critical web application security risks. Next, move on to other less critical vulnerabilities. Follow available guidance on securing web applications. [8] [9] [10]

How do I respond to unauthorized access to election-related systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.gov or 888-282-0870) or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

Resources

- CISA Tip: Best Practices for Securing Election Systems
- CISA Tip: Securing Voter Registration Data
- CISA Tip: Website Security
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Securing Network Infrastructure Devices
- Joint Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity

TLP:WHITE

- CISA Insights: Actions to Counter Email-Based Attacks on Election-related Entities
- FBI and CISA Public Service Announcement (PSA): Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- FBI and CISA PSA: Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- FBI and CISA PSA: Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- FBI and CISA PSA: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- FBI and CISA PSA: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Result

2. NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies" https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
3. https://owasp.org/www-project-dependency-check/
4. https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/defending-against-the-exploitation-of-sql-vulnerabilities-to.cfm
5. NSA & ASD "CyberSecurity Information: Detect and Prevent Web Shell Malware" https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
6. https://us-cert.cisa.gov/cdm/event/Identifying-and-Protecting-High-Value-Assets-Closer-Look-Governance-Needs-HVAs
7. NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies" https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf
8. NSA "Building Web Applications – Security for Developers" https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/building-web-applications-security-recommendations-for.cfm
9. https://owasp.org/www-project-top-ten/
10. https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Revisions

October 30, 2020: Initial Version
November 3, 2020: Updated IOC disclaimer to emphasize that only activity listed in this alert warrants further investigation.

Alert (AA20-296B)

More Alerts

Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems

Original release date: October 22, 2020

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are warning that Iranian advanced persistent threat (APT) actors are likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process.

The APT actors are creating fictitious media sites and spoofing legitimate media sites to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud.

The APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, structured query language (SQL) injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns.

Click here for a PDF version of this report.

Technical Details

These actors have conducted a significant number of intrusions against U.S.-based networks since August 2019. The actors leveraged several Common Vulnerabilities and Exposures (CVEs)—notably CVE-2020-5902 and CVE-2017-9248—pertaining to virtual private networks (VPNs) and content management systems (CMSs).

- CVE-2020-5902 affects F5 VPNs. Remote attackers could exploit this vulnerability to execute arbitrary code. [1].
- CVE-2017-9248 affects Telerik UI. Attackers could exploit this vulnerability in web applications using Telerik UI for ASP.NET AJAX to conduct cross-site scripting (XSS) attacks.[2]

Historically, these actors have conducted DDoS attacks, SQL injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns. These activities could render these systems temporarily inaccessible to the public or election officials,

which could slow, but would not prevent, voting or the reporting of results.

- **A DDoS attack** could slow or render election-related public-facing websites inaccessible by flooding the internet-accessible server with requests; this would prevent users from accessing online resources, such as voting information or non-official voting results. In the past, cyber actors have falsely claimed DDoS attacks have compromised the integrity of voting systems in an effort to mislead the public that their attack would prevent a voter from casting a ballot or change votes already cast.
- **A SQL injection** involves a threat actor inserting malicious code into the entry field of an application, causing that code to execute if entries have not been sanitized. SQL injections are among the most dangerous and common exploits affecting websites. A SQL injection into a media company's CMS could enable a cyber actor access to network systems to manipulate content or falsify news reports prior to publication.
- **Spear-phishing messages** may not be easily detectible. These emails often ask victims to fill out forms or verify information through links embedded in the email. APT actors use spear phishing to gain access to information—often credentials, such as passwords—and to identify follow-on victims. A malicious cyber actor could use compromised email access to spread disinformation to the victims' contacts or collect information sent to or from the compromised account.
- **Public-facing website defacements** typically involve a cyber threat actor compromising the website or its associated CMS, allowing the actor to upload images to the site's landing page. In situations where such public-facing websites relate to elections (e.g., the website of a county board of elections), defacements could cast doubt on the security and legitimacy of the websites' information. If cyber actors were able to successfully change an election-related website, the underlying data and internal systems would remain uncompromised..
- **Disinformation campaigns** involve malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, or discredit the electoral system. Malicious actors often use social media as well as fictitious and spoofed media sites for these campaigns. Based on their corporate policies, social media companies have worked to counter these actors' use of their platforms to promote fictitious news stories by removing the news stories, and in many instances, closing the accounts related to the malicious activity. However, these adversaries will continue their attempts to create fictitious accounts that promote divisive storylines to sow discord, even after the election.

Mitigations

The following recommended mitigations list includes self-protection strategies against the cyber techniques used by the APT actors:

- Validate input—input validation is a method of sanitizing untrusted input provided by web application users. Implementing input validation can protect against security flaws of web applications by significantly reducing the probability of successful exploitation. Types of attacks possibly prevented include SQL injection, XSS, and command injection.

- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP; do not have open RDP ports, unless there is a valid business reason to do so. Place any system with an open RDP port behind a firewall, and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- Apply multi-factor authentication, when possible.
- Apply system and software updates regularly, particularly if you are deploying products affected by CVE-2020-5902 and CVE-2017-9248.
  - For patch information on CVE-2020-5902, refer to F5 Security Advisory K52145254.
  - For patch information on CVE-2017-9248, refer to Progress Telerik details for CVE-2017-9248.
- Maintain a good information back-up strategy that involves routinely backing up all critical data and system configuration information on a separate device. Store the backups offline; verify their integrity and restoration process.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days, and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access are required to follow internal policies on remote access.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as VPNs, recognizing VPNs are only as secure as the connected devices.
- Be aware of unsolicited contact on social media from any individual you do not know.
- Be aware of attempts to pass links or files via social media from anyone you do not know.
- Be aware of unsolicited requests to share a file via online services.
- Be aware of email messages conveying suspicious alerts or other online accounts, including login notifications from foreign countries or other alerts indicating attempted unauthorized access to your accounts.
- Be suspicious of emails purporting to be from legitimate online services (e.g., the images in the email appear to be slightly pixelated and/or grainy, language in the email seems off, the email originates from an IP address not attributable to the provider/company).
- Be suspicious of unsolicited email messages that contain shortened links (e.g., via `tinyurl`, `bit.ly`).

- Use security features provided by social media platforms, use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches; automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed at which threat actors create exploits after a patch is released. These "N-day" exploits can be as damaging as a zero-day exploits. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to ensure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.[3] In addition to updating the application, use tools (e.g., the OWASP Dependency-Check Project tool[4]) to identify publicly known vulnerabilities in third-party libraries that the application depends on.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (SQL injection, cross-site scripting, etc.); use a commercial web application vulnerability scanner in combination with a source code scanner.[5] As vulnerabilities are found, they should be fixed or patched. This is especially crucial for networks that host older web applications; as sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

Deploy a web application firewall (WAF) to help prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware.[6] Malicious cyber actors often deploy web shells—software that can enable remote administration—on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands, which are commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, with remote access, and/or used on high value assets.[7] Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs).[8] Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remedite critical web application security risks first; then, move on to other less critical vulnerabilities. Follow available guidance on securing web applications.[9],[10],[11]

How do I respond to unauthorized access to election-related systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.dhs.gov or 888-282-0870) or the Federal Bureau of Investigation (FBI) through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

Resources

- CISA Tip: Best Practices for Securing Election Systems
- CISA Tip: Securing Voter Registration Data
- CISA Tip: Website Security
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- CISA Tip: Securing Network Infrastructure Devices
- CISA Activity Alert: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Insights: Actions to Counter Email-Based Attacks On Election-related Entities
- FBI and CISA Public Service Announcement (PSA): Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
- FBI and CISA PSA: Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
- FBI and CISA PSA: Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
- FBI and CISA PSA: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
- FBI and CISA PSA: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting

- FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results

TLP:WHITE

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

References

[1] F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
[2] Progress Telerik details for CVE-2017-9248
[3] NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies
[4] OWASP Dependency-Check
[5] NSA "Defending Against the Exploitation of SQL Vulnerabilities to Compromis…
[6] NSA & ASD "CyberSecurity Information: Detect and Prevent Web Shell Malware"
[7] CISA: Identifying and Protecting High Value Assets: A Closer Look at Govern…
[8] NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies"
[9] NSA "Building Web Applications – Security for Developers":
[10] OWASP Top Ten
[11] 2020 CWE Top 25 Most Dangerous Software Weaknesses

Revisions

October 22, 2020: Initial Version

Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated September 18, 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 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 elections infrastructure subsector (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. However, DHS does provide cyber vulnerability assessments and risk mitigation guidance to political campaigns upon request as resources permit.

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 and the EAC, as well as secretaries of state, lieutenant governors, and elections officials who altogether represent 24 state and local governments. It also includes non-voting members from other relevant federal agencies. 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 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. 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. DHS is currently drafting an SSP for the EIS.

The CI designation for election infrastructure is also intended to facilitate use of existing resources, such as

- *Cybersecurity and Infrastructure Security Agency (CISA)*. CISA, an agency within DHS, serves as the SSA for the EIS.

- *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 CISA, 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.

Brian E. Humphreys, bhumphreys@crs.loc.gov, 7-0975

IF10677

TLP:WHITE

Alert (AA20-283A)

More Alerts

APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

Original release date: October 09, 2020 | Last revised: October 24, 2020

Summary

This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

Note: the analysis in this joint cybersecurity advisory is ongoing, and the information provided should not be considered comprehensive. The Cybersecurity and Infrastructure Security Agency (CISA) will update this advisory as new information is available.

This joint cybersecurity advisory was written by CISA with contributions from the Federal Bureau of Investigation (FBI).

CISA has recently observed advanced persistent threat (APT) actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability—CVE-2020-1472—in Windows Netlogon. The commonly used tactic, known as vulnerability chaining, exploits multiple vulnerabilities in the course of a single intrusion to compromise a network or application.

This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks. Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.

CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.

Some common tactics, techniques, and procedures (TTPs) used by APT actors include leveraging legacy network access and virtual private network (VPN) vulnerabilities in association with the recent critical CVE-2020-1472 Netlogon vulnerability. CISA is aware of multiple cases where the Fortinet FortiOS Secure Socket Layer (SSL) VPN vulnerability CVE-2018-13379 has been exploited to gain access to networks. To a lesser extent, CISA has also observed threat actors exploiting the MobileIron vulnerability CVE-2020-15505. While these exploits have been observed recently, this activity is ongoing and still unfolding.

After gaining initial access, the actors exploit CVE-2020-1472 to compromise all Active Directory (AD) identity services. Actors have then been observed using legitimate remote access tools, such as VPN and Remote Desktop Protocol (RDP), to access the environment with the compromised credentials. Observed activity targets multiple sectors and is not limited to SLTT entities.

CISA recommends network staff and administrators review internet-facing infrastructure for these and similar vulnerabilities that have or could be exploited to a similar effect, including Juniper CVE-2020-1631, Pulse Secure CVE-2019-11510, Citrix NetScaler CVE-2019-19781, and Palo Alto Networks CVE-2020-2021 (this list is not considered exhaustive).

Click here for a PDF version of this report.

Technical Details

Initial Access

APT threat actors are actively leveraging legacy vulnerabilities in internet-facing infrastructure (*Exploit Public-Facing Application* [T1190], *External Remote Services* [T1133]) to gain initial access into systems. The APT actors appear to have predominately gained initial access via the Fortinet FortiOS VPN vulnerability CVE-2018-13379.

Although not observed in this campaign, other vulnerabilities, listed below, could be used to gain network access (as analysis is evolving, these listed vulnerabilities should not be considered comprehensive). As a best practice, it is critical to patch all known vulnerabilities within internet-facing infrastructure.

- Citrix NetScaler CVE-2019-19781
- MobileIron CVE-2020-15505
- Pulse Secure CVE-2019-11510
- Palo Alto Networks CVE-2020-2021
- F5 BIG-IP CVE-2020-5902

Fortinet FortiOS SSL VPN CVE-2018-13379

CVE-2018-13379 is a path traversal vulnerability in the FortiOS SSL VPN web portal. An unauthenticated attacker could exploit this vulnerability to download FortiOS system files through specially crafted HTTP resource requests. [1]

MobileIron Core & Connector Vulnerability CVE-2020-15505

CVE-2020-15505 is a remote code execution vulnerability in MobileIron Core & Connector versions 10.3 and earlier. [2] This vulnerability allows an external attacker, with no privileges, to execute code of their choice on the vulnerable system. As mobile device management (MDM) systems are critical to configuration management for external devices, they are usually highly permissioned and make a valuable target for threat actors.

Privilege Escalation

Post initial access, the APT actors use multiple techniques to expand access to the environment. The actors are leveraging CVE-2020-1472 in Windows Netlogon to escalate privileges and obtain access to Windows AD servers. Actors are also leveraging the opensource tools such as Mimikatz and the CrackMapExec tool to obtain valid account credentials from AD servers (*Valid Accounts* [T1078]).

Microsoft Netlogon Remote Protocol Vulnerability: CVE-2020-1472

CVE-2020-1472 is a vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory.[3] This vulnerability could allow an unauthenticated attacker with network access to a domain controller to completely compromise all AD identity services (*Valid Accounts: Domain Accounts* [T1078.002]). Malicious actors can leverage this vulnerability to compromise other devices on the network (*Lateral Movement* [TA0008]).

Persistence

Once system access has been achieved, the APT actors use abuse of legitimate credentials (*Valid Accounts* [T1078]) to log in via VPN or remote access services *(External Remote Services* [T1133]) to maintain persistence.

Mitigations

Organizations with externally facing infrastructure devices that have the vulnerabilities listed in this joint cybersecurity advisory, or other vulnerabilities, should move forward with an "assume breach" mentality. As initial exploitation and escalation may be the only observable exploitation activity, most mitigations will need to focus on more traditional network hygiene and user management activities.

Keep Systems Up to Date

Patch systems and equipment promptly and diligently. Establishing and consistently maintaining a thorough patching cycle continues to be the best defense against adversary TTPs. See table 1 for patch information on CVEs mentioned in this report.

Table 1: Patch information for CVEs

Vulnerability	Vulnerable Products	Patch Information
CVE-2018-13379	• FortiOS 6.0: 6.0.0 to 6.0.4 • FortiOS 5.6: 5.6.3 to 5.6.7 • FortiOS 5.4: 5.4.6 to 5.4.12	• Fortinet Security Advisory: FG-IR-18-384
CVE-2019-19781	• Citrix Application Delivery Controller • Citrix Gateway • Citrix SDWAN WANOP	• Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 • Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 • Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 • Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5
CVE-2020-5902	• Big-IP devices (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	• F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
CVE-2019-11510	• Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 • Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	• Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX
CVE-2020-15505	• MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0 • Sentry versions 9.7.2 and earlier, and 9.8.0; • Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier	• MobileIron Blog: MobileIron Security Updates Available
CVE-2020-1631	• Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1	• Juniper Security Advisory JSA11021
CVE-2020-2021	• PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL)	• Palo Alto Networks Security Advisory for CVE-2020-2021

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-1472	• Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2012 • Windows Server 2012 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2019 (Server Core installation) • Windows Server, version 1903 (Server Core installation) • Windows Server, version 1909 (Server Core installation) • Windows Server, version 2004 (Server Core installation)	• Microsoft Security Advisory for CVE-2020-1472

Comprehensive Account Resets

If there is an observation of CVE-2020-1472 Netlogon activity or other indications of valid credential abuse detected, it should be assumed the APT actors have compromised AD administrative accounts, the AD forest should not be fully trusted, and, therefore, a new forest should be deployed. Existing hosts from the old compromised forest cannot be migrated in without being rebuilt and rejoined to the new domain, but migration may be done through "creative destruction," wherein as endpoints in the legacy forest are decommissioned, new ones can be built in the new forest. This will need to be completed on on-premise as well as Azure-hosted AD instances.

Note that fully resetting an AD forest is difficult and complex; it is best done with the assistance of personnel who have successfully completed the task previously.

It is critical to perform a full password reset on all user and computer accounts in the AD forest. Use the following steps as a guide.

1. Create a temporary administrator account, and use this account only for all administrative actions
2. Reset the Kerberos Ticket Granting Ticket (`krbtgt`) password [4]; this must be completed before any additional actions (a second reset will take place in step 5)
3. Wait for the krbtgt reset to propagate to all domain controllers (time may vary)
4. Reset all account passwords (passwords should be 15 characters or more and randomly assigned):
    a. User accounts (forced reset with no legacy password reuse)
    b. Local accounts on hosts (including local accounts not covered by Local Administrator Password Solution [LAPS])
    c. Service accounts
    d. Directory Services Restore Mode (DSRM) account
    e. Domain Controller machine account
    f. Application passwords
5. Reset the `krbtgt` password again
6. Wait for the `krbtgt` reset to propagate to all domain controllers (time may vary)
7. Reboot domain controllers
8. Reboot all endpoints

The following accounts should be reset:

- AD Kerberos Authentication Master (2x)
- All Active Directory Accounts
- All Active Directory Admin Accounts
- All Active Directory Service Accounts

- All Active Directory User Accounts
- DSRM Account on Domain Controllers
- Non-AD Privileged Application Accounts
- Non-AD Unprivileged Application Accounts
- Non-Windows Privileged Accounts
- Non-Windows User Accounts
- Windows Computer Accounts
- Windows Local Admin

CVE-2020-1472

To secure your organization's Netlogon channel connections:

- **Update all Domain Controllers and Read Only Domain Controllers**. On August 11, 2020, Microsoft released software updates to mitigate CVE-2020-1472. Applying this update to domain controllers is currently the only mitigation to this vulnerability (aside from removing affected domain controllers from the network).
- **Monitor for new events, and address non-compliant devices** that are using vulnerable Netlogon secure channel connections.
- **Block public access to potentially vulnerable ports**, such as 445 (Server Message Block [SMB]) and 135 (Remote Procedure Call [RPC]).

To protect your organization against this CVE, follow advice from Microsoft, including:

- Update your domain controllers with an update released August 11, 2020, or later.
- Find which devices are making vulnerable connections by monitoring event logs.
- Address non-compliant devices making vulnerable connections.
- Enable enforcement mode to address CVE-2020-1472 in your environment.

VPN Vulnerabilities

Implement the following recommendations to secure your organization's VPNs:

- **Update VPNs, network infrastructure devices, and devices** being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Software Updates and Securing Network Infrastructure Devices. Wherever possible, enable automatic updates. See table 1 for patch information on VPN-related CVEs mentioned in this report.
- **Implement multi-factor authentication (MFA) on all VPN connections to increase security**. Physical security tokens are the most secure form of MFA, followed by authenticator app-based MFA. SMS and email-based MFA should only be used when no other forms are available. If MFA is not implemented, require teleworkers to use strong passwords. See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.

Discontinue unused VPN servers. Reduce your organization's attack surface by discontinuing unused VPN servers, which may act as a point of entry for attackers. To protect your organization against VPN vulnerabilities:

- **Audit** configuration and patch management programs.
- **Monitor** network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., Secure Shell [SSH], SMB, RDP).
- **Implement** MFA, especially for privileged accounts.
- **Use** separate administrative accounts on separate administration workstations.
- **Keep** software up to date. Enable automatic updates, if available.

How to uncover and mitigate malicious activity

- **Collect and remove** for further analysis:
  - Relevant artifacts, logs, and data.
- **Implement** mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.
- **Consider** soliciting incident response support from a third-party IT security organization to:
  - Provide subject matter expertise and technical support to the incident response.

- Ensure that the actor is eradicated from the network.
- Avoid residual issues that could result in follow-up compromises once the incident is closed.

Resources

- CISA VPN-Related Guidance
- CISA Infographic: Risk Vulnerability And Assessment (RVA) Mapped to the MITRE ATT&CK FRAMEWORK
- National Security Agency InfoSheet: Configuring IPsec Virtual Private Networks
- CISA Joint Advisory: AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Activity Alert: AA20-073A: Enterprise VPN Security
- CISA Activity Alert: AA20-031A: Detecting Citrix CVE-2019-19781
- CISA Activity Alert: AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability
- **Cybersecurity Alerts and Advisories**: Subscriptions to CISA Alerts and MS-ISAC Advisories

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- CISA (888-282-0870 or Central@cisa.dhs.gov), or
- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office

References

[1] Fortinet Advisory: FG-IR-18-384
[2] MobileIron Blog: MobileIron Security Updates Available
[3] Microsoft Security Advisory for CVE-2020-1472
[4] Microsoft: AD Forest Recovery - Resetting the krbtgt password

Revisions

October 9, 2020: Initial Version
October 11, 2020: Updated Summary
October 12, 2020: Added Additional Links

Press Releases

Treasury Continues Pressure on Maduro Regime for Role in Fraudulent Elections

December 18, 2020

Washington – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Ex-Cle Soluciones Biometricas C.A. (Ex-Cle C.A.) for materially supporting the illegitimate President of Venezuela Nicolas Maduro Moros, including by providing goods and services that the Maduro regime used to carry out the fraudulent December 6, 2020 parliamentary elections. In addition, OFAC designated Guillermo Carlos San Agustin and Marcos Javier Machado Requena for having acted for or on behalf of Ex-Cle Soluciones Biometricas C.A.

"The illegitimate Maduro regime's efforts to steal elections in Venezuela show its disregard for the democratic aspirations of the Venezuelan people," said Secretary Steven T. Mnuchin. "The United States remains committed to targeting the Maduro regime and those who support its aim to deny the Venezuelan people their right to free and fair elections."

This entity and individuals were designated pursuant to Executive Order (E.O.) 13692, as amended.

EX-CLE SOLUCIONES BIOMETRICAS C.A.

Ex-Cle Soluciones Biometricas C.A. (Ex-Cle C.A.), a Venezuelan-registered biometric technology company, operates in Venezuela as the subsidiary of Argentine-registered Ex-Cle S.A. The parent company opened an office in Venezuela in 2004 to provide management solutions for government entities, including to Maduro's National Electoral Council (CNE – Consejo Nacional Electoral). In May 2016, the parent company began operating in Venezuela under the name Ex-Cle C.A., and since then, Ex-Cle C.A. has been doing business as the electoral hardware and software vendor with Maduro regime-aligned government agencies and officials. In addition, Ex-Cle C.A. has assisted the CNE in purchasing thousands of voting machines from foreign vendors, which were transshipped through Tehran, Iran, via Mahan Air and Conviasa, both previously sanctioned by OFAC. Ex-Cle C.A. has contracts worth millions of dollars with the Maduro regime.

GUILLERMO CARLOS SAN AGUSTIN

Guillermo Carlos San Agustin (San Agustin), a dual Argentine and Italian national, is a co-director, the administrator, a majority shareholder, and ultimate beneficial owner of Ex-Cle C.A. San Agustin is partnered in Ex-Cle C.A. with Marcos Javier Machado Requena, a Venezuelan national, and Carlos Enrique Quintero Cuevas (Quintero), previously designated by OFAC, who is an alternate CNE rector and member of the Venezuelan military, and is the primary day-to-day

manager of the procurement and electoral corruption activity from inside the CNE on behalf of Ex-Cle C.A.

MARCOS JAVIER MACHADO REQUENA

Marcos Javier Machado Requena (Machado), a Venezuelan national, is a co-director, the president, and a minority shareholder of Ex-Cle C.A. Machado is involved in the management and financial operations of procurement of election-related voting machines and hardware procured from foreign vendors for the Government of Venezuela, and is partnered with San Agustin and Quintero in running Ex-Cle C.A. out of Caracas.

Today, Ex-Cle C.A. was designated pursuant to E.O. 13692 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Maduro. In addition, San Agustin and Machado were designated pursuant to E.O. 13692 for having acted or purported to act for or on behalf of, directly or indirectly, Ex-Cle C.A.

As a result of today's action, all property and interests in property of the persons designated today that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by the designated persons are also blocked. OFAC's regulations generally prohibit all dealings by U.S. persons or those within (or transiting) the United States that involve any property or interests in property of blocked or designated persons.

U.S. sanctions need not be permanent; sanctions are intended to bring about a positive change of behavior. The United States has made clear that the removal of sanctions may be available for individuals and entities, including those designated pursuant to E.O. 13692, who take concrete and meaningful actions to stop providing support to the illegitimate Maduro regime, including to those Government of Venezuela agencies that support him.

View identifying information on the entity designated today.

116TH CONGRESS
1st Session

SENATE

REPORT
116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE

WITH ADDITIONAL VIEWS

CONTENTS

Russian Efforts Against Election Infrastructure

I. (U) INTRODUCTION

(U) From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

II. (U) FINDINGS

1. [redacted] The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure[1] at the state and local level. [redacted] The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.[2]

2. [redacted]

---

[1] **(U)** The Department of Homeland Security (DHS) defines *election infrastructure* as "storage facilities, polling places, and centralized vote tabulation 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," according to the January 6, 2017 statement issued by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, available at https://www.dhs.gov/news/2017/10/06/statement-secretary-johnson-designation-election-infrastructure-critical. Similarly, the Help America Vote Act (HAVA), Pub. L. No. 107-252, Section 301(b)(1) refers to a functionally similar set of equipment as "voting systems," although the definition excludes physical polling places themselves, among other differences, 52 U.S.C. §21081(b). This report uses the term *election infrastructure* broadly, to refer to the equipment, processes, and systems related to voting, tabulating, reporting, and registration.

[2] [redacted] The Committee has reviewed the intelligence reporting underlying the Department of Homeland Security (DHS) assessment from early 2017 [redacted] The Committee finds it credible.

[3] **(U)** The names of the states the Committee spoke to have been replaced with numbers. DHS and some states asked the Committee to protect state names before providing the Committee with information. The Committee's goal was to get the most information possible, so state names are anonymized throughout this report. Where the report refers to public testimony by Illinois state election officials, that state is identified.

3. **(U)** While the Committee does not know with confidence what Moscow's intentions were, Russia may have been probing vulnerabilities in voting systems to exploit later. Alternatively, Moscow may have sought to undermine confidence in the 2016 U.S. elections simply through the discovery of their activity.

4. **(U)** Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The U.S. intelligence apparatus is, by design, foreign-facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.

5. **(U)** DHS and FBI alerted states to the threat of cyber attacks in the late summer and fall of 2016, but the warnings did not provide enough information or go to the right people. Alerts were actionable, in that they provided malicious Internet Protocol (IP) addresses to information technology (IT) professionals, but they provided no clear reason for states to take this threat more seriously than any other alert received.

6. **(U)** In 2016, officials at all levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impression they were trying to dispel—that the voting systems were insecure.

7. **(U)** Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain.

8. **(U)** In the face of this threat and these security gaps, DHS has redoubled its efforts to build trust with states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning how election procedures vary across states and how federal entities can be of most help to states. The U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and other groups have helped DHS in this effort. DHS's work to bolster states' cybersecurity has likely been effective, in particular for those states that have leveraged DHS's cybersecurity assessments for election infrastructure, but much more needs to be done to coordinate state, local, and federal knowledge and efforts in order to harden states' electoral infrastructure against foreign meddling.

9. **(U)** To assist in addressing these vulnerabilities, Congress in 2018 appropriated $380 million in grant money for the states to bolster cybersecurity and replace vulnerable

voting machines.[4] When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.

10. **(U)** DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. States should be firmly in the lead for running elections. The country's decentralized election system can be a strength from a cybersecurity perspective, but each operator should be keenly aware of the limitations of their cybersecurity capabilities and know how to quickly and properly obtain assistance.

III. (U) THE ARC OF RUSSIAN ACTIVITIES

[redacted] In its review of the 2016 elections, the Committee found no evidence that vote tallies were altered or that voter registry files were deleted or modified, though the Committee and IC's insight into this is limited. Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections [redacted] Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities targeting the voting process. [redacted] the Committee found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes.[5]

[redacted]

- [redacted]

---

[4] **(U)** Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 561-562.
[5] **(U)** The Committee has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases. These activities are routinely carried out in the context of private sector breaches.
[6] [redacted] FBI LHM, [redacted]
[7] [redacted] FBI LHM, [redacted]
[8] [redacted] DHS Homeland Intelligence Brief, [redacted]
[9] [redacted] FBI LHM, [redacted]

- [redacted]
- [redacted]

[redacted] Evidence of scanning of state election systems first appeared in the summer prior to the 2016 election. In mid-July 2016, Illinois discovered anomalous network activity, specifically a large increase in outbound data, on a Illinois Board of Elections' voter registry website.[12] Working with Illinois, the FBI commenced an investigation.[13] [redacted] The attack resulted in data exfiltration from the voter registration database.[16]

(U) On August 18, 2016, FBI issued an unclassified FLASH[17] to state technical-level experts on a set of [redacted] suspect IP addresses identified from the attack on Illinois's voter registration databases.[18] [redacted] The FLASH product did not attribute the attack to Russia or any other particular actor.[21]

---

[10] **(U/[redacted])** FBI Electronic Communication, [redacted]

[11] [redacted] FBI LHM, [redacted]

[12] **(U)** DHS briefing for SSCI staff, March 5, 2018.

[13] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 113.

[14] **(U[redacted])** According to the United States Computer Emergency Readiness Team (US-CERT), an SQL injection is "an [redacted] technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code."

[15] **(U)** DHS IIR 4 0050006 17, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016

[16] **(U[redacted])** DHS briefing for SSCI staff, March 5, 2018.

[17] **(U)** FBI FLASH alerts are notifications of potential cyber threats sent to local law enforcement and private industry so that administrators are able to guard their systems against the described threat. FLASHs marked TLP: AMBER are considered sharable with members of the recipients own organization and those with direct need to know.

[18] [redacted] Number T-LD1004-TT, TLP-AMBER, [redacted]

[19] **(U)** *Ibid.*

[20] **(U)** *Ibid.*

[21] R[redacted]wned

(U[redacted]) After the issuance of the August FLASH, the Department of Homeland Security (DHS) and the Multi-State-Information Sharing & Analysis Center (MS-ISAC)[22] asked states to review their log files to determine if the IP addresses described in the FLASH had touched their infrastructure. This request for voluntary self-reporting, in conjunction with DHS analysis of NetFlow activity on MS-ISAC internet sensors, identified another 20 states whose networks had made connections to at least one IP address listed on the FLASH.[23] DHS was almost entirely reliant on states to self-report scanning activity.

[redacted] Former Special Assistant to the President and Cybersecurity Coordinator Michael Daniel said, "eventually we get enough of a picture that we become confident over the course of August of 2016 that we're seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure on a regular basis."[25] Dr. Samuel Liles, Acting Director of the Cyber Analysis Division within DHS's Office of Intelligence and Analysis (I&A), testified to the Committee on June 21, 2017, that "by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors."[26]

[redacted]

[22] (U) The MS-ISAC is a DHS-supported group dedicated to sharing information between state, local, tribal, and territorial (SLTT) government entities. It serves as the central cybersecurity resource for SLTT governments. Entities join to receive cybersecurity advisories and alerts, vulnerability assessments, incident response assistance, and other services.

[23] (U[redacted]) DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Governments to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.

[24] (U) SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 41.

[25] (U) SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on August 31, 2017, p. 39.

[26] (U) SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 12.

(U) DHS and FBI issued a second FLASH and a Joint Analysis Report in October that flagged [redacted] suspect IP addresses, many unrelated to Russia.[27] DHS briefers told the Committee that they were intentionally over-reporting out of an abundance of caution, given their concern about the seriousness of the threat. DHS representatives told the Committee, "We were very much at that point in a sort of duty-to-warn type of attitude . . . where maybe a specific incident like this, which was unattributed at the time, wouldn't have necessarily risen to that level. But . . . we were seeing concurrent targeting of other election-related and political figures and political institutions . . . [which] led to what would probably be more sharing than we would normally think to do."[28]

[redacted]

[redacted] DHS assessed that the searches, done alphabetically, probably included all 50 states, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."[31]

[redacted]

---

[27] (U[redacted]) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

[28] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 9-10.

[29] [redacted] FBI LHM, [redacted]

[30] [redacted]

[31] [redacted] DHS Homeland Intelligence Brief, *Update:* [redacted]

[32] [redacted] NSA [redacted] DIRNSA, May 5, 2017. This information was not available to the U.S. government until April 2017.

[33] [redacted]

[34] (U) NSA [redacted] DIRNSA, May 5, 2017.

[redacted] The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[37] In objecting to these tactics, then-Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland reminded the Russian Ambassador that Russia had refused invitations to participate in the official OSCE mission that was to observe the U.S. elections.[38]

[redacted]

[35] (U) FBI IIR [redacted]; FBI IIR [redacted]
[36] (U) *Ibid.*
[37] (U) DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 221-222.
[38] [redacted] Email, sent November 4, 2016; from [redacted]; to: [redacted]. Subject: Kislyak Protest of FBI Tactics.
[39] (U) NSA [redacted] DIRNSA, May 5, 2017.
[40] (U) *Ibid.*
[41] [redacted]
[42] [redacted]
[43] [redacted]

(U) The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election Day, though again the Committee and IC's insight into this is limited.

(U[redacted]) In the years since the 2016 election, awareness of the threat, activity by DHS, and measures at the state and local level to better secure election infrastructure have all shown considerable improvement. The threat, however, remains imperfectly understood. In a briefing before Senators on August 22, 2018, DNI Daniel Coats, FBI Director Christopher Wray, then-DHS Secretary Kirstjen Nielsen, and then-DHS Undersecretary for the National Protection and Programs Division Christopher Krebs told Senators that there were no known threats to election infrastructure. However, Mr. Krebs also said that top election vulnerabilities remain, including the administration of the voter databases and the tabulation of the data, with the latter being a much more difficult target to attack.[44] Relatedly, several weeks prior to the 2018 mid-term election, DHS assessed that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election."[45]

[redacted]

IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES

A. (U) Targeting Activity

[redacted] Scanning of election-related state infrastructure by Moscow was the most widespread activity the IC and DHS elements observed in the run up to the 2016 election.[48]

- [redacted] In an interview with the Committee, Mr. Daniel stated: "What it mostly looked like to us was reconnaissance. . . . I would have characterized it at the time as sort of conducting the reconnaissance to do the network mapping, to do the topology mapping so

---

[44] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[45] (U[redacted]) Homeland Security Intelligence Assessment: Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018.
[46] (U) DTS 2019-1368, NIC 2019-01, Intelligence Community Assessment: A Summary of the Intelligence Community Report on Foreign Interference as Directed by Executive Order 13848, March 29, 2019. p. 2-3.
[47] (U) *Ibid.*
[48] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 12.

that you could actually understand the network, establish a presence so you could come back later and actually execute an operation."[49]

- **(U)** Testifying before the Committee, Dr. Liles characterized the activity as "simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in . . . [however] a small number of the networks were successfully exploited. They made it through the door."[50]

[redacted] DHS and FBI assessments on the number of affected states evolved since 2016. In a joint FBI/DHS intelligence product published in March 2018, and coordinated with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Department of State, the National Intelligence Council, the National Security Agency (NSA), and the Department of Treasury, DHS and FBI assessed [redacted] that Russian intelligence services conducted activity [redacted].[51] [redacted]

- [redacted] DHS arrived at their initial assessment by evaluating whether the tactics, techniques, and procedures (TTPs) observed were consistent with previously observed Russian TTPs, whether the actors used known Russian-affiliated malicious infrastructure, and whether a state or local election system was the target.[53]

- **(U)** The majority of information examined by DHS was provided by the states themselves. The MS-ISAC gathered information from states that noticed the suspect IPs pinging their systems. In addition, FBI was working with some states in local field offices and reporting back FBI's findings.

- **(U)** If some states evaluated their logs incompletely or inaccurately, then DHS might have no indication of whether they were scanned or attacked. As former-Homeland Security Adviser Lisa Monaco told the Committee, "Of course, the law enforcement and the intelligence community is going to be significantly reliant on what the holders and

---

[49] **(U)** SSCI Transcript of the Interview of Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 44.
[50] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[51] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]
[52] **(U)** *See* chart, *infra*, for information on successful breaches.
[53] **(U)** DHS did not count attacks on political parties, political organizations, or NGOs. For example, the compromise of an email affiliated with a partisan State 13 voter registration organization was not included in DHS's count.

owners and operators of the infrastructure sees on its system [sic] and decides to raise their hand."[54]

[redacted] However, both the IC and the Committee in its own review were unable to discern a pattern in the affected states, [redacted]

(U) Mr. Daniel told the Committee that by late August 2016, he had already personally concluded that the Russians had attempted to intrude in all 50 states, based on the extent of the activity and the apparent randomness of the attempts. "My professional judgment was we have to work under the assumption that they've tried to go everywhere, because they're thorough, they're competent, they're good."[55]

[redacted] Intelligence developed later in 2018 bolstered Mr. Daniel's assessment that all 50 states were targeted. [redacted]

- [redacted]

---

[54] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 38.
[55] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 40.
[56] [redacted] DHS/FBI Homeland Intelligence Bulletin, [redacted]
[57] **(U)** *Ibid.*
[58] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[59] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, pp. 11-12.
[60] **(U)** DHS briefing for SSCI staff, March 5, 2018.

- [redacted]
- [redacted]

[redacted]

(U) However, IP addresses associated with the August 18, 2016 FLASH provided some indications the activity might be attributable to the Russian government, particularly the GRU:

- [redacted]
- [redacted]
- (U[redacted]) One of the Netherlands-based [redacted] "exhibited the same behavior from the same node over a period of time. . . . It was behaving like . . . the same user or group of users was using this to direct activity against the same type of targets," according to DHS staff.[69]

---

[61] (U) *Ibid.*
[62] (U) *Ibid.*
[63] (U) *Ibid.*
[64] (U) *Ibid.*
[65] [redacted]
[66] [redacted] FBI IIR [redacted]
[67] (U) Cyber Threat Intelligence Integration Center (CTIIC) Cyber Threat Intelligence Summary, October 7, 2016.
[68] (U) *Ibid.*
[69] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

- [redacted]

[redacted] The IC's confidence level about the attribution of the attacks evolved over 2017 and into 2018. [redacted]

- [redacted]

- [redacted]

[redacted] The Committee reached out to the 21 states that DHS first identified as targets of scanning activity to learn about their experiences. Election officials provided the Committee

---

[70] (U) DHS Electronic Communication, December 19, 2016, email from: DHS/NCCIC; to: CIA.
[71] [redacted]
[72] [redacted]
[73] [redacted] DHS Intelligence Assessment, *Hostile Russian Cyber Targeting of Election Infrastructure in 2016; Probable Non-State Actors Attempt Disruption*, May 3, 2017.
[74] (U) *Ibid.*
[75] (U) SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.
[76] [redacted] DHS arrived at their initial assessment of 21 states affected by adding the eleven plus seven states, plus the three where scanning activity appeared directed at less specifically election-focused infrastructure.
[77] (U) SSCI conference call with DHS and FBI, March 29, 2018.

details about the activity they saw on their networks, and the Committee compared that accounting to DHS's reporting of events.[78] Where those accounts differed is noted below. The scanning activity took place from approximately June through September 2016.

STATE	OBSERVED ACTIVITY[79]
Illinois	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 2	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 3	**(U)** According to State 3 officials, cyber actors using infrastructure identified in the August FLASH conducted scanning activity.[80] State 3 officials noticed "abnormal behavior" and took action to block the related IP addresses.[81] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[82]
State 4	**(U)** *See infra,* "Two Unexplained Events" for a detailed description.
State 5	**(U)** Cyber actors using infrastructure identified in the August FLASH scanned "an old website and non-relevant archives," according to the State 5 Secretary of State's office.[83] The following day, State 5 took action to block the IP address.[84] [redacted] DHS, however, reported GRU scanning activity on two separate State 5 Secretary of State websites, plus targeting of a District Attorney's office[85] in a particular city.[86] Both the websites appear to be current addresses for the State 5 Secretary of State's office.
State 6	**(U)** According to State 6 officials, cyber actors using infrastructure identified in the August FLASH scanned[87] the entire state IT infrastructure, including by using the Acunetix tool, but the "affected systems" were the Secretary of State's

[78] **(U)** DHS briefed Committee staff three times on the attacks, and staff reviewed hundreds of pages of intelligence assessments.

[79] **(U)** Slight variation between what states and DHS reported to the Committee is an indication of one of the challenges in election cybersecurity. The system owners—in this case, state and local administrators—are in the best position to carry out comprehensive cyber reviews, but they often lack the expertise or resources to do so. The federal government has resources and expertise, but the IC can see only limited information about inbound attacks because of legal restrictions on operations inside the United States.

[80] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

[81] **(U)** *Ibid.*

[82] **(U)** DHS briefing for Committee staff on March 5, 2018.

[83] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

[84] **(U)** *Ibid.*

[85] **(U/[redacted])** Briefers suggested the "most wanted" list housed on the District Attorney's website may have in some way been connected to voter registration. The exact nature of this connection, including whether it was a technical network connection or whether databases of individuals with felony convictions held by the District Attorney's office had voting registration implications, is unclear.

[86] **(U)** DHS briefing for Committee staff on March 5, 2018.

[87] **(U)** State 6 officials did not specify, but in light of the DHS assessment, they likely meant SQL injection.

	web application and the election results website.[88] If the penetration had been successful, actors could have manipulated the unofficial display of the election tallies.[89] State officials believed they would have caught any inconsistency quickly.[90] State 6 became aware of this malicious activity and alerted partners.[91] [redacted] DHS reported that GRU actors scanned State 6, then unsuccessfully attempted many SQL injection attacks. State 6 saw the highest number of SQL attempts of any state.
State 7	**(U)** According to State 7 officials, cyber actors using infrastructure identified in the August FLASH scanned public-facing websites, including the "static" election site.[92] It seemed the actors were "cataloging holes to come back later," according to state election officials.[93] State 7 became aware of this malicious activity after receiving an FBI alert.[94] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[95]
State 8	**(U)** According to State 8 officials, cyber actors using infrastructure identified in the August FLASH scanned a State 8 public election website on one day.[96] State 8 officials described the activity as heightened but not particularly out of the ordinary.[97] State 8 became aware of this malicious activity after receiving an alert.[98] [redacted]
State 9	**(U)** According to State 9 officials, cyber actors using infrastructure identified in an October MS-ISAC advisory[101] scanned the statewide voter registration

[88] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[89] **(U)** *Ibid.*
[90] **(U)** *Ibid.*
[91] **(U)** *Ibid.*
[92] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[93] **(U)** *Ibid.*
[94] **(U)** *Ibid.*
[95] **(U)** DHS briefing for Committee staff on March 5, 2018.
[96] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[97] **(U)** *Ibid.*
[98] **(U)** *Ibid.*
[99] **(U)** DHS briefing for Committee staff on March 5, 2018.
[100] **(U)** *Ibid.*
[101] **(U)** While the Committee was unable to review the specific indicators shared with State 9 by the MS-ISAC in October, the Committee believes at least one of the relevant IPs was originally named in the August FLASH because of technical data held by DHS which was briefed to the Committee.

	system.[102] Officials used the analogy of a thief casing a parking lot: they said the car thief "didn't go in, but we don't know why."[103] State 9 became aware of this malicious activity after receiving an alert.[104] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[105]
State 10	**(U)** According to State 10 officials, cyber actors using infrastructure identified in the August FLASH conducted activity that was "very loud," with a three-pronged attack: a Netherlands-based IP address attempted SQL injection on all fields 1,500 times, a U.S.-based IP address attempted SQL injection on several fields, and a Poland-based IP address attempted SQL injection on one field 6-7 times.[106] State 10 received relevant cybersecurity indictors from MS-ISAC in early August, around the same time that the attacks occurred.[107] State 10's IT contractor attributed the attack to Russia and suggested that the activity was reminiscent of other attacks where attackers distract with lots of noise and then "sneak in the back."[108] **(U)** State 10, through its firewall, blocked attempted malicious activity against the online voter registration system and provided logs to the National Cybersecurity and Communications Integration Center (NCCIC)[109] and the U.S. Computer Emergency Readiness Team (US-CERT).[110] State 10 also brought in an outside contractor to assist.[111] [redacted] DHS confirmed GRU SQL injection attempts against State 10's voter services website on August 5 and said that the attack was blocked after one day by State 10's firewall.[112]
State 11	**(U)** According to State 11 officials, they have seen no evidence of scanning or attack attempts related to election infrastructure in 2016.[113] While State 11 officials noted an IP address "probing" state systems, activity which was "broader than state election systems," State 11 election officials did not provide specifics on which systems.[114]

[102] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[103] **(U)** *Ibid.*
[104] **(U)** *Ibid.*
[105] **(U)** DHS briefing for Committee staff on March 5, 2018.
[106] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 10], November 29, 2017.
[107] **(U)** *Ibid.*
[108] **(U)** *Ibid.*
[109] **(U)** NCCIC is DHS's cyber watch center.
[110] **(U)** *Ibid.*
[111] **(U)** *Ibid.*
[112] **(U)** DHS briefing for Committee staff on March 5, 2018.
[113] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[114] **(U)** *Ibid.*

	[redacted] DHS reported GRU scanning activity on the Secretary of State domain.[115]
State 12	**(U)** Cyber actors using infrastructure identified in the August FLASH conducted scanning activity that "lasted less than a second and no security breach occurred," according to State 12 officials.[116] State 12 became aware of this malicious activity after being alerted to it.[117] [redacted] DHS reported that because of a lack of sensor data related to this incident, they relied on NetFlow data, which provided less granular information.[118] DHS's only clear indication of GRU scanning on State 12's Secretary of State website came from State 12 self-reporting information to MS-ISAC after the issuance of the August FLASH notification.[119]
State 13	**(U)** According to State 13 officials, they have seen no evidence of scanning or attack attempts related to state-wide election infrastructure in 2016.[120] [redacted]
State 14	[redacted] MS-ISAC passed DHS reports of communications between a suspect IP address used by the GRU at the time and the State 14 election commission webpage, but no indication of a compromise.[123] In addition, DHS was informed of activity relating to separate IP addresses in the August FLASH,

[115] **(U)** DHS briefing for Committee staff on March 5, 2018.
[116] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[117] **(U)** *Ibid.*
[118] **(U)** DHS briefing for Committee staff on March 5, 2018.
[119] **(U)** *Ibid.*
[120] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[121] **(U)** FBI IIR [redacted] DHS briefing for Committee staff on March 5, 2018.
[122] [redacted]; DHS briefing for Committee staff on March 5, 2018. For more information on decisions by DHS to exclude certain activity in its count of 21 states, *see* text box, *infra*, "DHS Methodology for Identifying States Touched by Russian Cyber Actors."
[123] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]; DHS briefing for Committee staff on March 5, 2018.

	including attempted Domain Name System (DNS) lookups and potentially malicious emails, some dating back to January 2016.[124]
State 15	**(U)** State 15 officials were not aware that the state was among those targeted until they were notified.[125] State 15's current lead election official was not in place during the 2016 election so they had little insight into any scanning or attempted intrusion on their systems. State 15 officials said that generally they viewed 2016 as a success story because the attempted infiltration never got past the state's four layers of security. [redacted] DHS reported broad GRU scanning activity on State 15 government domains.[126]
State 16	**(U)** According to State 16 officials, cyber actors using infrastructure identified in the October FLASH conducted scanning activity against a state government network.[127] [redacted] DHS reported information on GRU scanning activity based on a self-report from State 16 after the issuance of the October FLASH.[128]
State 17	**(U)** State 17 officials reported nothing "irregular, inconsistent, or suspicious" leading up to the election.[129] While State 17 IT staff received an MS-ISAC notification, that notification was not shared within the state government.[130] [redacted] DHS reported GRU scanning activity on an election-related domain.[131]
State 18	**(U)** State 18 election officials said they observed no connection from the IP addresses listed in the election-related notifications.[132] [redacted] DHS reported indications of GRU scanning activity on a State 18 government domain.[133]
State 19	**(U)** According to State 19 officials, cyber actors using infrastructure identified in October by MS-ISAC conducted scanning activity. State 19 claimed this activity was "blocked," but did not elaborate on why or how it was blocked.[134]

[124] **(U/[redacted])** DHS IIR 4 019 0012 17, *Cyber Activity Targeting [State 14] Government Networks from Internet Protocol Addresses Associated with Targeting State Elections Systems*, October 21, 2016.
[125] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 15], March 12, 2018.
[126] **(U)** DHS briefing for Committee staff on March 5, 2018.
[127] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[128] **(U)** DHS briefing for Committee staff on March 5, 2018.
[129] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[130] **(U)** *Ibid.*
[131] **(U)** DHS briefing for Committee staff on March 5, 2018.
[132] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 18], December 8, 2017.
[133] **(U)** DHS briefing for Committee staff on March 5, 2018.
[134] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 19], December 1, 2017.

	[redacted] DHS reported indications of GRU scanning activity on two separate State 19 government domains.[135]
State 20	**(U)** According to State 20 officials, cyber actors using infrastructure identified in October by MS-ISAC were "knocking" on the state's network, but no successful intrusion occurred.[136] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[137]
State 21	**(U)** State 21 officials received indicators from MS-ISAC in October 2016. They said they were not aware the state was among those targeted until notified.[138] [redacted] DHS reported GRU scanning activity on an election-related domain as well as at least one other government system connected to the voter registration system.[139]

[redacted] Neither DHS nor the Committee can ascertain a pattern to the states targeted, lending credence to DHS's later assessment that all 50 states probably were scanned. DHS representatives told the Committee that "there wasn't a clear red state-blue state-purple state, more electoral votes, less electoral votes" pattern to the attacks. DHS acknowledged that the U.S. Government does not have perfect insight, and it is possible the IC missed some activity or that states did not notice intrusion attempts or report them.[140] [redacted]

[redacted]

[135] **(U)** DHS briefing for Committee staff on March 5, 2018.
[136] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[137] **(U)** DHS briefing for Committee staff on March 5, 2018.
[138] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.
[139] **(U)** DHS briefing for Committee staff on March 5, 2018.
[140] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 25.
[141] [redacted]
[142] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p..21.

(U/[redacted]) As of October 2018, the IC and DHS were looking for evidence of threats to election systems, [redacted]. An October 11, 2018 DHS Intelligence Assessment reported the following:

> *We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018, although we do not have a complete baseline of prior years to determine relative scale of the activity. Much of our understanding of cyber threats to election infrastructure is due to proactive sharing by state and local election officials, as well as more robust intelligence and information sharing relationships amongst the election community and within the Department. The observed activity has leveraged common tactics—the types of tactics that are available to nation-state and non-state cyber actors, alike—with limited success in compromising networks and accounts. We have not attributed the activity to any foreign adversaries, and we continue to work to identify the actors behind these operations. At this time, all these activities were either prevented or have been mitigated.*

(U/[redacted]) Specifically:

> *Unidentified cyber actors since at least April 2018 and as recently as early October continue to engage in a range of potential elections-related cyber incidents targeting election infrastructure using spear-phishing, database exploitation techniques, and denial of service attacks, possibly indicating continued interest in compromising the availability, confidentiality, and integrity of these systems. For example, on 24 August 2018, cybersecurity officials detected multiple attempts to illegally access the State of Vermont's Online Voter Registration Application (OLVR), which serves as the state's resident voter registration database, according to DHS reporting. The malicious activity included one Cross Site Scripting attempt, seven Structured Query Language (SQL) injection attempts, and one attempted Denial of Service (DoS) attack. All attempts were unsuccessful.*[143]

(U/[redacted]) In summarizing the ongoing threat to U.S. election systems, DHS further said in the same product, "We continue to assess multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions."[144]

B. (U) Russian Access to Election Infrastructure

---

[143] (U/[redacted]) DHS, Homeland Security Intelligence Assessment, *Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure*, October 11, 2018.
[144] (U) *Ibid.*

(U) The January 6, 2017 Intelligence Community Assessment (ICA), "Assessing Russian Activities and Intentions in Recent U.S. Elections," states:

> *Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.*[145]

[redacted] Based on the Committee's review of the ICA, the Committee concurs with this assessment. The Committee found that Russian-affiliated cyber actors gained access to election infrastructure systems across two states, including successful extraction of voter data. However, none of these systems were involved in vote tallying.

1. (U) Russian Access to Election Infrastructure: Illinois

(U) In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the 2016 election.[146] As of the end of 2018, the Russian cyber actors had successfully penetrated Illinois's voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records.[147] The compromise resulted in the exfiltration of an unknown quantity of voter registration data.[148] Russian cyber actors were in a position to delete or change voter data, but the Committee is not aware of any evidence that they did so.[149]

- [redacted] DHS assesses with high confidence that the penetration was carried out by Russian actors.[150]
- (U[redacted]) The compromised voter registration database held records relating to 14 million registered voters, [redacted]. The records exfiltrated included information on each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number.[151]

---

[145] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. iii.
[146] **(U[redacted])** DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.
[147] **(U)** "Illinois election officials say hack yielded information on 200,000 voters," [Local Newspaper], August 29, 2016.
[148] **(U)** DHS IIR [redacted] SCI Open Hearing on June 21, 2017, p 110
[149] **(U)** State Board of Elections, *Illinois Voter Registration System Records Breached*, August 31, 2016. As reflected elsewhere in this report, the Committee did not undertake its own forensic analysis of the Illinois server logs to corroborate this statement; SSCI interview with DHS and CTIIC, February 27, 2018, p. 24.
[150] **(U)** *See infra*, "Russian Scanning and Attempted Access to Election-Related Infrastructure" for a complete discussion on attribution related to the set of cyber activity linked to the infrastructure used in the Illinois breach.
[151] **(U[redacted])** FBI IIR [redacted] DHS Intelligence Assessment, May 3, 2017, 0144-17, p. 2.

- [redacted] DHS staff further recounted to the Committee that "Russia would have had the ability to potentially manipulate some of that data, but we didn't see that."[152] Further, DHS staff noted that "the level of access that they gained, they almost certainly could have done more. Why they didn't . . . is sort of an open-ended question. I think it fits under the larger umbrella of undermining confidence in the election by tipping their hand that they had this level of access or showing that they were capable of getting it."[153]

- **(U)** According to a Cyber Threat Intelligence Integration Center (CTIIC) product, Illinois officials "disclosed that the database has been targeted frequently by hackers, but this was the first instance known to state officials of success in accessing it."[154]

(U) In June 2017, the Executive Director of the Illinois State Board of Elections (SBE), Steve Sandvoss, testified before the Committee about Illinois's experience in the 2016 elections.[155] He laid out the following timeline:

- **(U)** On June 23, 2016, a foreign actor successfully penetrated Illinois's databases through an SQL attack on the online voter registration website. "Because of the initial low-volume nature of the attack, the State Board of Election staff did not become aware of it at first."[156]

- **(U)** Three weeks later, on July 12, 2016, the IT staff discovered spikes in data flow across the voter registration database server. "Analysis of the server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of our paperless online voter application website."[157]

- **(U)** On July 13, 2016, IT staff took the website and database offline, but continued to see activity from the malicious IP address.[158]

- **(U)** "Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th [2016], when they abruptly ceased."[159]

---

[152] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 14.
[153] **(U)** *Ibid.*
[154] **(U)** CTIIC Cyber Threat Intelligence Summary, August 18, 2016.
[155] **(U)** SSCI Open Hearing on June 21, 2017. The Committee notes that, in his testimony, Mr. Sandvoss said Illinois still had not been definitively told that Russia perpetrated the attack, despite DHS's high confidence. The Committee also notes that DHS eventually provided a briefing to states during which DHS provided further information on this topic, including the DHS high-confidence attribution to Russia.
[156] **(U)** *Ibid.*, p. 110.
[157] **(U)** *Ibid.*
[158] **(U)** *Ibid.*, p. 111.
[159] **(U)** *Ibid.*

- **(U)** On July 19, 2016, the election staff notified the Illinois General Assembly and the Attorney General's office.
- **(U)** Approximately a week later, the FBI contacted Illinois.[160]
- **(U)** On July 28, 2016, both the registration system and the online voter registration became fully functional again.[161]

2. (U) Russian Access to Election Infrastructure: State 2

[redacted] Separately, GRU cyber actors breached election infrastructure in State 2. [redacted]

- [redacted]

---

[160] **(U)** *Ibid.*, p. 113.
[161] **(U)** *Ibid.*, p. 112.
[162] **(U)** [redacted] FBI Electronic Communication, [redacted]
[163] **(U)** *Ibid.*
[164] [redacted]
[165] **(U)** FBI Briefing on [State 2] Election Systems, June 25, 2018.
[166] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[167] **(U)** *Ibid.*
[168] **(U)** *Ibid.*
[169] **(U)** *Ibid.*
[170] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 16.
[171] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, compartmented session.

[redacted]

(U) FBI and DHS Interactions with State 2[179]	
August 18, 2016	(U) FBI FLASH notification identified IP addresses targeting election offices.[180]
August 24, 2016	(U) State 2 Department of State received the FLASH from National Association of Secretaries of State.[181]
August 26, 2016	(U) State 2 Department of State forwarded FLASH to counties and advised them to block the IP addresses.[182] [redacted] Separately, [redacted] determined one of the listed IP addresses scanned its system.[183] [redacted] subsequently discovered suspected intrusion activity and contacted the FBI.[184]

[172] (U) *Ibid.*
[173] (U) *Ibid.*
[174] (U) *Ibid.*
[175] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[176] (U) *Ibid.*
[177] [redacted] *Ibid. See also* EB-0004893-LED
[178] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 42.
[179] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[180] (U) FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[181] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 4.
[182] (U) *Ibid.*, pp. 4-5.
[183] (U) *Ibid.*, p. 5.
[184] (U) *Ibid.*

August 31, 2016	[redacted] FBI opened its investigation on the [redacted] and "conducted outreach to State 2 county election officials to discuss individual security postures and any suspicious activity."[185] FBI outreach reveals that one State 2 county—County A—was scanned.[186]
September 30, 2016	[redacted] FBI held a conference call with county election officials to advise of the attempt to probe County A.[187] FBI also notified state and local officials of available DHS services.[188]
October 4, 2016	[redacted] County B's IT administrator contacted FBI regarding a potential intrusion.[189] According to the FBI, "Of particular concern, the activity included a connection to a county voting, testing, and maintenance server used for poll worker classes."[190]
October 14, 2016	(U) FBI shared County B indicators by issuing a FLASH.[191]
December 29, 2016	(U) DHS and FBI released a Joint Analysis Report (JAR) on the "GRIZZLY STEPPE" intrusion set; report represents the first IC attribution of state election-related systems to the Russians.[192]
[redacted]	[redacted]
June 2017	(U) DHS notified State 2 counties of a possible intrusion "as part of a broader notification to 122 entities identified as spearphishing victims in an intelligence report."[194]

[185] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 5.
[186] (U) *Ibid.*
[187] (U) *Ibid.*, pp. 5-6.
[188] (U) *Ibid.*, p. 6.
[189] (U) *Ibid.*
[190] (U) *Ibid.*
[191] (U[redacted]) FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]
[192] (U) DHS/FBI, Joint Analysis Report, JAR-16-20296A, GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.
[193] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[194] (U) *Ibid.*

July 2017	**(U)** FBI published a FLASH report warning of possible spearphishing.[195]
November 2017	**(U)** FBI and DHS participated in the first meeting of the State 2 elections task force.[196]
February 2018	**(U)** FBI requested direct engagement with Counties B, C, and D, including a reminder of available DHS services.[197]
March 2018	**(U)** FBI reports that "our office engaged" the affected counties through the local FBI field office.[198] The FBI could not provide any further detail on the substance of these engagements to the Committee.
May 29, 2018	[redacted] FBI provided a SECRET Letterhead Memo to DHS "formally advising of our investigation into the intrusion [redacted], the reported intrusion at County B, and suspected compromises of Counties C and D."[199]
June 11, 2018	**(U)** FBI reports that as of June 11, 2018, Counties A, B, C, and D had not accepted DHS services.[200]

[redacted]

[redacted]

[195] **(U)** FBI FLASH, Alert Number EB-000083-LD, TLP-AMBER, [redacted]. *See* DTS 2018-3174.
[196] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[197] **(U)** *Ibid.*, p. 6.
[198] **(U)** *Ibid.*, p. 34.
[199] **(U)** *Ibid.*, pp. 8-9.
[200] **(U)** *Ibid.*, p. 20.
[201] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 20-21.
[202] [redacted] DHS briefing for SSCI staff, March 5, 2018.

- **(U)** State 2's Secretary of State and Election Director told the Committee in December 2017 that there was "never an attack on our systems." "We did not see any unusual activities. I would have known about it personally."[203] State 2 did not want to share with the Committee its cybersecurity posture, but state officials communicated that they are highly confident in the security of their systems.[204]

- **(U)** State 2's election apparatus is highly decentralized, with each county making its own decisions about acquiring, configuring, and operating election systems.[205]

- **(U)** As of August 9, 2018, DHS was complimentary of the steps State 2 had taken to secure its voting systems, including putting nearly all counties on the ALBERT sensor system, joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and using congressionally appropriated funds plus additional state funds to hire cybersecurity advisors.[206]

C. (U) Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure

[redacted]

- [redacted]

---

[203] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 2], December 1, 2017.
[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** DTS 2018-2581, Memorandum for the Record, Telephone call with DHS, August 9, 2018.
[207] [redacted] FBI LHM, [redacted]
[208] **(U)** *Ibid.*, p. 5.
[209] [redacted] Note: "FISA" refers to electronic surveillance collected on a foreign power or an agent of a foreign power pursuant to the Foreign Intelligence Surveillance Act of 1978. This collection could have come from landlines, electronic mail accounts, or mobile phones used by personnel at a foreign embassy (i.e., an "establishment" FISA) or used by personnel associated with a foreign power (i.e., "agents of a foreign power"). This FISA collection would have been approved by the Foreign Intelligence Surveillance Court ("FISC"), effectuated by FBI, and then could also have been shared with NSA or CIA, or both, depending on the foreign target.

[redacted]

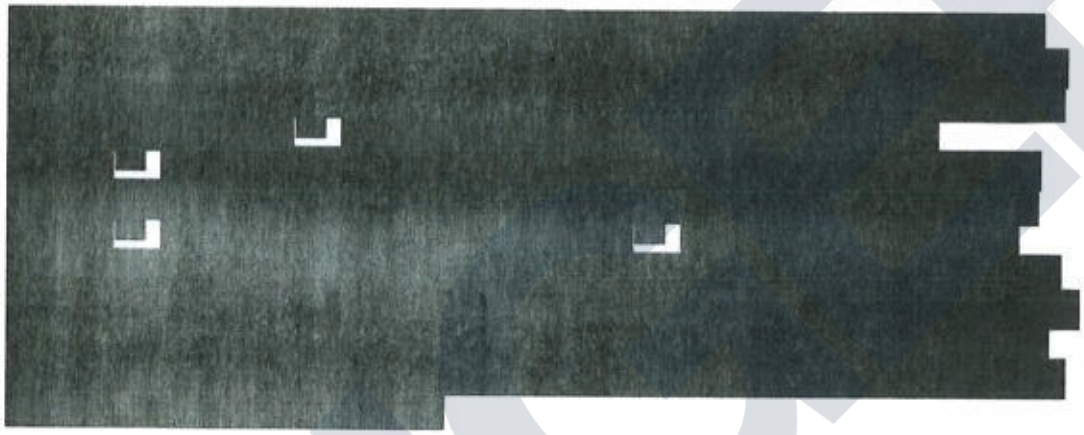
- [redacted]
- [redacted] It is unknown if Tarantsov attended the events.
- [redacted]
- [redacted]

D. (U) Russian Activity Directed at Voting Machine Companies

---

[210] [redacted] FBI LHM, [redacted]
[211] FBI LHM, [redacted]
[212] **(U)** *Ibid.*
[213] **(U)** *Ibid.*, p. 3.
[214] **(U)** *Ibid.*, p. 4.
[215] **(U)** *Ibid.*
[216] **(U)** *Ibid.*, p. 5.
[217] [redacted]

Russian government actors engaged in attacks on election systems,

- FBI reported that "between December 2015 and June 2016, DHS further told the Committee that malicious cyber actors had scanned a widely-used vendor of election systems.[219]
- 

E. (U) Russian Efforts to Observe Polling Places

Department of State were aware that Russia was attempting to send election observers to polling places in 2016. The true intention of these efforts is unknown.

- 

---

[218] FBI Electronic Communication,

[219] (U) DHS briefing for SSCI staff, March 5, 2018.

[220]

[221] (U) *Ibid.*

[222] (U) *Ibid.*

[223] (U) NSA DIRNSA, May 5, 2017, p. 3.

[224] (U) *Ibid.*, pp. 1-3.

[225] (U) FBI IIR

[226] (U) *Ibid.*

- [redacted] The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[227] For example, in September 2016, the State 5 Secretary of State denied a request by the Russian Consul General to allow a Russian government official inside a polling station on Election Day to study the U.S. election process, according to State 5 officials.[228] [redacted]

[redacted] n mission.[231]

[redacted] nterfere

- [redacted]

---

[227] (U) DTS 2018-2152, SSCI Transcript of the Interview of Andrew McCabe, Former Deputy Director of the Federal Bureau of Investigation, February 14, 2018, pp. 221-222.
[228] (U) *Ibid.*
[229] (U) *Ibid.*
[230] (U) *Ibid.*
[231] [redacted] Email, sent November 4, 2016; from [redacted]; to: [redacted]; subject: Kislyak Protest of FBI Tactics.
[232] [redacted] Email, sent: September 13, 2016; from; [redacted] subject: Russia visas/travel.
[233] (U) *Ibid.*
[234] (U) *Ibid.*
[235] [redacted] Email Sent: Monday, November 7, 2016, 8:11 AM; from: [redacted]; to: [redacted] subject: RE: Kislyak Protest of FBI Tactics --- SECRET//NOFORN.

F.

G. (U) Russian Activity Possibly Related to a Misinformation Campaign on Voter

---

[236] DTS 2018-3952; MFR of Interview with Randy Coleman, December 5, 2018.
[237] (U) NSA DIRNSA, May 5, 2017.
[238] (U) *Ibid.*
[239] (U) SSCI Interview with DHS and CTIIC, February 27, 2018, pp. 47-48.
[240] FBI IIR
[241] (U/) FBI LHM,
[242] (U) *Ibid.*

[redacted]

(U) The declassified, January 6, 2017, Intelligence Community Assessment also highlighted preparations related to voter fraud, noting that Russian diplomats "were prepared to publicly call into question the validity of the results" and that "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."[245]

(U) During a 2017 election, State 17 saw bot activity on social media, including allegations of voter fraud, in particular on Reddit. State 17 had to try to prove later that there was no fraud.[246]

H. (U) Two Unexplained Events

1. (U) Cyber Activity in State 22

[redacted]

---

[243] [redacted]

[244] [redacted]

[245] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. 2.

[246] **(U)** *See* Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018. The Committee notes it is conducting a related investigation into the use of social media by Russian-government affiliated entities.

[247] **(U)** The Fusion Center model is a partnership between DHS and state, local, tribal, and territorial entities. They serve as a focal point for "the receipt, analysis, gathering, and sharing of threat-related information."

[248] **(U)** CTIIC Cyber Threat Intelligence Summary/Cyber Threats in Focus, Malicious Cyber Activity on Election-Related Computer Networks Last Spring Possibly Linked to Russia, October 7, 2016; DHS, IIR 4 019 0147 16, September 28, 2016.

[249] **(U)** *Ibid.*

[250] **(U)** *Ibid.*

2. (U) Cyber Activity in State 4

(U[redacted]) State 4 officials, DHS, and FBI in the spring and summer of 2016, struggled to understand who was responsible for two rounds of cyber activity related to election infrastructure. Eventually, one set of cyber activity was attributed to Russia and one was not.

(U[redacted]) First, in April of 2016, a cyber actor successfully targeted State 4 with a phishing scam. After a county employee opened an infected email attachment, the cyber actor stole credentials, which were later posted online.[251] Those stolen credentials were used in June 2016 to penetrate State 4's voter registration database.[252] A CTIIC product reported the incident as follows: "An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware, according to a private-sector DHS partner claiming secondhand access. The actor used the credentials to access the database and was in a position to modify county, but not statewide, data."[253]

(U[redacted]) DHS analysis of forensic data provided by a private sector partner discovered malware on the system, and State 4 shut down the voter registration system for about eight days to contain the attack.[254] State 4 officials later told the Committee that that while the cyber actor was able to successfully log in to a workstation connected to election related infrastructure, additional credentials would have been needed for the cyber actor to access the voter registration database on that system.[255]

(U) At first, FBI told State 4 officials that the attack may have originated from Russia, but the ties to the Russian government were unclear. "The Bureau described the threat as 'credible' and significant, a spokesman for State 4 Secretary of State said."[256] State 4 officials also told press that the hacker had used a server in Russia, but that the FBI could not confirm the

---

[251] (U) [redacted]

[252] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 38.

[253] [redacted] Cyber Threat Intelligence Integration Center (CTIIC), Compromised State Election Networks, November 2, 2016, p. 1.

[254] (U[redacted]) DHS IIR 4 005 0829 16, *A* [redacted] *U.S. State Government's Election System Targeted by Malicious Activity*, September 9, 2016; Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[255] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[256] (U) [redacted]

attack was tied to the Russian government.[257] DHS and FBI later assessed it to be criminal activity, with no definitive tie to the Russian government.[258]

[redacted] Subsequently, Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library.[259] Officials saw no effective penetration of the system. DHS has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections.[260] [redacted]

V. (U) RUSSIAN INTENTIONS

(U) Russian intentions regarding U.S. election infrastructure remain unclear. Russia might have intended to exploit vulnerabilities in election infrastructure during the 2016 elections and, for unknown reasons, decided not to execute those options. Alternatively, Russia might have sought to gather information in the conduct of traditional espionage activities. Lastly, Russia might have used its activity in 2016 to catalog options or clandestine actions, holding them for use at a later date. Based on what the IC knows about Russia's operating procedures and intentions more broadly, the IC assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy.

- (U) Former-Homeland Security Adviser Lisa Monaco told the Committee that "[t]here was agreement [in the IC] that one of the motives that Russia was trying to do with this active measures campaign was to sow distrust and discord and lack of confidence in the voting process and the democratic process."[262]

- [redacted] DHS representatives told the Committee that "[w]e see . . . Russians in particular obviously, gain access, learn about the environment, learn about what systems are interconnected, probing, the type of intelligence preparation of the environment that you would expect from an actor like the Russians. So certainly the context going forward

---

[redacted]

[258] (U) SSCI interview with DHS and CTIIC, February 27, 2018, p. 40.
[259] (U) [redacted]
[260] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]
[261] (U) *Ibid.*
[262] (U) SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 30.

is a concern of what they might have learned and how much more they know about the systems."[263]

- [redacted] Mr. McCabe told the Committee that it seemed to him like "classic Russian cyber espionage. . . . [They will] scrape up all the information and the experience they possibly can," and "they might not be effective the first time or the fifth time, but they are going to keep at it until they can come back and do it in an effective way."[264]

- [redacted] Mr. Daniel told the Committee:

> *While any one voting machine is fairly vulnerable, as has been demonstrated over and over again publicly, the ability to actually do an operation to change the outcome of an election on the scale you would need to, and do it surreptitiously, is incredibly difficult. A much more achievable goal would be to undermine confidence in the results of the electoral process, and that could be done much more effectively and easily. . . . A logical thing would be, if your goal is to undermine confidence in the U.S. electoral system—which the Russians have a long goal of wanting to put themselves on the same moral plane as the United States . . . one way would be to cause chaos on election day. How could you start to do that? Mess with the voter registration databases.*[265]

- [redacted] Ms. Monaco further echoed that concern:

> *Well, one of the things I was worried about—and I wasn't alone in this—is kind of worst-case scenarios, which would be things like the voter registration databases. So if you're a state and local entity and your voter registration database is housed in the secretary of state's office and it is not encrypted and it's not backed up, and it says Lisa Monaco lives at Smith Street and I show up at my [polling place] and they say 'Well we don't have Ms. Monaco at Smith Street, we have her at Green Street,' now there's difficulty in my voting. And if that were to happen on a large scale, I was worried about confusion at polling places, lack of confidence in the voting system, anger at a large scale in some areas, confusion, distrust. So there was a whole sliding scale of*

---

[263] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 15.
[264] **(U)** DTS 2018-2152, SSCI Transcript of the Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 224-225.
[265] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, pp. 27, 34.

horribles just when you're talking about voter registration databases.[266]

- [redacted]

(U) Chaos on Election Day: Three Scenarios

[redacted] Mr. Daniel said that in the early fall of 2016, a policy working group was looking at three scenarios:

> *One was, could the Russians do something to the voter registration databases that could cause problems on Election Day? An example of that would be, could you go in and flip the digits in everybody's address, so that when they show up with their photo ID it doesn't match what's in the poll book? It doesn't actually prevent people from voting. In most cases you'll still get a provisional ballot, but if this is happening in a whole bunch of precincts for just about everybody showing up, it gives the impression that there's chaos.*[268]
>
> *A second one was to do a variant of the penetrating voting machines, except this time what you do is you do a nice video of somebody conducting a hack on a voting machine and showing how you could do that hack and showing them changing a voting outcome, and then you post that on YouTube and you claim you've done this 100,000 times across the United States, even though you haven't actually done it at all.*[269]
>
> *Then the third scenario that we looked at was conducting a denial of service attack on the Associated Press on Election Day, because pretty much everybody, all those nice maps that everybody puts up on all the different news services, is in fact actually based on Associated Press stringers at all the different precincts and locations. . . . It doesn't actually change anything, but it gives the impression that there's chaos.*[270]

---

[266] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 28.

[267] [redacted]

[268] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 33.

[269] **(U)** *Ibid.*, pp. 34-35.

[270] **(U)** *Ibid.*, p. 35.

VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES

(U) In its review, the Committee has seen no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted, although the Committee and IC's insight is limited. Poll workers and voting monitors did not report widespread suspicious activity surrounding the 2016 election. DHS Assistant Secretary Jeanette Manfra said in the Committee's open hearing in June 2017 that "I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." Further, all three witnesses in that hearing—Ms. Manfra, Dr. Liles, and FBI Assistant Director for Counterintelligence Bill Priestap—agreed that they had no evidence that votes themselves were changed in any way in the 2016 election.[271]

- **(U)** Dr. Liles said that DHS "assessed that multiple checks and redundancies in U.S. election infrastructure, including diversity of systems, non-internet connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit, and validate the results—all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected."[272] He later said "the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection."[273]
- [redacted]
- **(U)** States did not report either an uptick in voters showing up at the polls and being unable to vote or a larger than normal quantity of provisional ballots.

(U) The Committee notes that nationwide elections are often won or lost in a small number of precincts. A sophisticated actor could target efforts at districts where margins are already small, and disenfranchising only a small percentage of voters could have a disproportionate impact on an election's outcome.

(U) Many state election officials emphasized their concern that press coverage of, and increased attention to, election security could create the very impression the Russians were seeking to foster, namely undermining voters' confidence in election integrity. Several insisted that whenever any official speaks publicly on this issue, they should state clearly the difference between a "scan" and a "hack," and a few even went as far as to suggest that U.S. officials stop

---

[271] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017.
[272] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[273] **(U)** *Ibid.*, p. 47.

talking about the issue altogether. One state official said, "We need to walk a fine line between being forthcoming to the public and protecting voter confidence."[274]

(U) Mr. Brennan described a similar concern in IC and policy discussions:

> *We know that the Russians had already touched some of the electoral systems, and we know that they have capable cyber capabilities. So there was a real dilemma, even a conundrum, in terms of what do you do that's going to try to stave off worse action on the part of the Russians, and what do you do that is going to . . . [give] the Russians what they were seeking, which was to really raise the specter that the election was not going to be fair and unaffected.*[275]

(U) Most state representatives interviewed by the Committee were confident that they met the threat effectively in 2016 and believed that they would continue to defeat threats in 2018 and 2020. Many had interpreted the events of 2016 as a success story: firewalls deflected the hostile activity, as they were supposed to, so the threat was not an issue. One state official told the Committee, "I'm quite confident our state security systems are pretty sound."[276] Another state official stated, "We felt good [in 2016]," and that due to additional security upgrades, "we feel even better today."[277]

(U) However, as of 2018, some states were still grappling with the severity of the threat. One official highlighted the stark contrast they experienced, when, at one moment, they thought elections were secure, but then suddenly were hearing about the threat.[278] The official went on to conclude, "I don't think any of us expected to be hacked by a foreign government."[279] Another official, paraphrasing a former governor, said, "If a nation-state is on the other side, it's not a fair fight. You have to phone a friend."[280]

(U) In the month before Election Day, DHS and other policymakers were planning for the worst-case scenario of efforts to disrupt the vote itself. Federal, state, and local governments created incident response plans to react to possible confusion at the polling places. Mr. Daniel said of the effort: "We're most concerned about the Russians, but obviously we are also concerned about the possibility for just plain old hacktivism on Election Day. . . . The incident response plan is actually designed . . . to help us [plan for] what is the federal government going to do if bad things start to happen on Election Day?"

[redacted] Mr. Daniel added that this was the first opportunity to exercise the process established under Presidential Policy Directive-41. "We asked the various agencies with lead

---

[274] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[275] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 54.
[276] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[277] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[278] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[279] **(U)** *Ibid.*
[280] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

responsibility, all right, give us your Election Day plan." That led to the creation of an Election Day playbook; steps included enhanced watch floor procedures, connectivity between FBI field offices and FBI and DHS, and an "escalation path" if "we needed to get to Lisa [Monaco] or Susan [Rice] in a hurry" on Election Day.[281]

VII. (U) SECURITY OF VOTING MACHINES

(U) The Committee review of Russian activity in 2016 highlighted potential vulnerabilities in many voting machines, with previous studies by security researchers taking on new urgency and receiving new scrutiny. Although researchers have repeatedly demonstrated it is possible to exploit vulnerabilities in electronic voting machines to alter votes,[282] some election officials dispute whether such attacks would be feasible in the context of an actual election.

- **(U)** Dr. Alex Halderman, Professor of Computer Science at the University of Michigan, testified before the Committee in June 2017 that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes."[283] Dr. Halderman concluded, "Voting machines are not as distant from the internet as they may seem."[284]

- **(U)** When State 7 decommissioned its Direct-Recording Electronic (DRE) voting machines in 2017, the IT director led an exercise in attempting to break into a few of the machines using the access a "normal" voter would have in using the machines.[285] The results were alarming: the programmed password on some of the machines was ABC123, and the testers were able to flip the machines to supervisor mode, disable them, and "do enough damage to call the results into question."[286] The IT director shared the results with State 21 and State 24, which were using similiar machines.[287]

- **(U)** In 2017, DEFCON[288] researchers were able to find and exploit vulnerabilities in five different electronic voting machines.[289] The WinVote machines, those recently decertified by State 7, were most easily manipulated. One attendee said, "It just took us a couple of hours on Google to find passwords that let us unlock the administrative

---

[281] **(U)** *Ibid.*, p. 82.
[282] **(U)** *See also, infra*, "Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities."
[283] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 117.
[284] **(U)** *Ibid.*, p. 110.
[285] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[286] **(U)** *Ibid.* The machines used were WinVote voting machines.
[287] **(U)** *Ibid.*
[288] **(U)** DEFCON is an annual hacker conference held in Las Vegas, Nevada. In July 2017, at DEFCON 25, the conference featured a Voting Machine Hacking Village ("Voting Village") which acquired and made available to conference participants over 25 pieces of election equipment, including voting machines and electronic poll books, for generally unrestricted examination for vulnerabilities.
[289] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, pp. 8-13.

functions on this machine."[290] A researcher was able to hack into the WinVote over WiFi within minutes using a vulnerability from 2003.[291] Once he had administrator-level access, he could change votes in the database. Researchers also discovered available USB ports in the machine that would allow a hacker to run software on the machine.[292] One said "with physical access to back [sic] of the machine for 15 seconds, an attacker can do anything."[293] Hackers were less successful with other types of machines, although each had recorded vulnerabilities.[294]

- **(U)** The 2018 DEFCON report found similar vulnerabilities, in particular when hackers had physical access to the machines. For example, hackers exploited an old vulnerability on one machine, using either a removable device purchasable on eBay or remote access, to modify vote counts.[295]

- **(U[redacted])** DHS briefed the Committee in August 2018 that these results were in part because the hackers had extended physical access to the machines, which is not realistic for a true election system. Undersecretary Krebs also disagreed with reporting that a 17-year-old hacker had accessed voter tallies.[296] Some election experts have called into question the DEFCON results for similar reasons and pointed out that any fraud requiring physical access would be, by necessity, small scale, unless a government were to deploy agents across thousands of localities.

- **(U)** ES&S Voting Systems disclosed that some of its equipment had a key security vulnerability. ES&S installed remote access software on machines it sold in the mid-2000s, which allowed the company to provide IT support more easily, but also created potential remote access into the machines. When pressed by Senator Ron Wyden of Oregon, the company admitted that around 300 voting jurisdictions had the software. ES&S says the software was not installed after 2007, and it was only installed on election-management systems, not voting machines.[297] More than 50 percent of voters vote on ES&S equipment, and 41 states use its products.

---

[290] **(U)** Elizabeth Wise, "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines," *USA Today*, July 30, 2017, https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.
[291] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, p. 4.
[292] **(U)** *Ibid.*, p. 9.
[293] **(U)** *Ibid.*
[294] **(U)** *Ibid.*, pp. 8-13.
[295] **(U)** Robert McMillian and Dustin Volz, "Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds," *Wall Street Journal*, September 27, 2018. The machine referenced is the ES&S Model 650, which ES&S stopped making in 2008 but is still available for sale.
[296] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018
[297] **(U)** Hacks, Security Gaps And Oligarchs: The Business of Voting Comes Under Scrutiny. Miles Parks, NPR, September 21, 2018.

(U) Advocates of electronic voting point out the flaws in paper ballots, like the potential for the introduction of fraudulent ballots or invalidated votes due to stains or extra marks. The Committee believes that any election system should be protected end-to-end, including against fraud.

(U) Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities

(U) While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a "recount" would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.[298]

(U) Dr. Halderman said in his June 2017 testimony before SSCI:

> *I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.*
>
> *Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at the time the most widely used touch-screen DRE in the country and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win.*[299]

---

[298] **(U)** "Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots." Written Statement by J. Alex Halderman, June 21, 2017, citing S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop,* August 2007; B. Campbell and M. Byrne, "Now do Voters Notice Review Screen Anomalies?" *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop,* August 2009.

[299] **(U)** The machine was the Diebold AccuVote TS, which was still used statewide in at least one state as of 2017.

> *Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in* every single case, *they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.*[300]

(U) In speaking with the Committee, federal government officials revealed concerns about the security of voting machines and related infrastructure. Former Assistant Attorney General for National Security John Carlin told the Committee:

> *"I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it, and the cooperation between some states and the federal government."*[301] *Mr. Carlin further stated, "We've literally seen it already, so shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think this was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be."*[302]

(U) Mr. McCabe echoed these concerns, and noted that, in the last months before the election, FBI identified holes in the security of election machines, saying "there's some potential there."[303]

(U) As of November 2016, five states were using exclusively DRE voting machines with no paper trail, according to open source information.[304] An additional nine states used at least some DRE voting machines with no paper trail.[305]

- **(U)** State 20 has 21-year-old DRE machines. While the state is in the process of replacing its entire voting system, including these machines, State 20 is aiming to have the updates ready for the 2020 elections.

- **(U)** In State 21, 50 of 67 counties as of November 2017 used DRE voting machines.[306]

---

[300] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, pp. 116-117.
[301] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, held on Monday, September 25, 2017, p. 86.
[302] **(U)** *Ibid.*, pp. 86-87.
[303] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, p. 221.
[304] **(U)** BallotPedia, *Voting Methods and Equipment By State*, https://ballotpedia.org/Voting_methods_and_equipment_by_state.
[305] **(U)** *Ibid.*
[306] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.

- **(U)** State 5 used paper-backed voting in only about half its machines and DRE voting machines without paper backup in the other half.[307]

- **(U)** Some states are moving to a hybrid model—an electronic voting machine with a paper backup, often in the form of a receipt that prints after the voter submits their vote. For example, State 12 uses some DREs, but all equipment is required to have a paper trail, and the paper ballot is the ballot of record.[308] State 12 also conducts a mandatory state-wide audit.[309] Similarly, State 13 uses some paper-based and some electronic machines, but all are required to have a paper trail.[310]

(U) The number of vendors selling voting machines is shrinking, raising concerns about a vulnerable supply chain. A hostile actor could compromise one or two manufacturers of components and have an outsized effect on the security of the overall system.

- [redacted] "My job," said Ms. Monaco when asked whether she was worried about voting machines themselves getting hacked, "was to worry about every parade of horribles. So I cannot tell you that that did not cross my mind. We were worried about who, how many makers. We were worried about the supply chain for the voting machines, who were the makers? . . . Turns out I think it's just Diebold—and have we given them a defensive briefing? So to answer your question, we were worried about it all."[311]

- [redacted] Mr. McCabe pointed out that a small number of companies have "90%" of the market for voting machines in the U.S. Before the 2016 election, [redacted] briefed a few of the companies on vulnerabilities,[312] but a more comprehensive campaign to educate vendors and their customers is warranted.

(U) Voluntary Voting System Guidelines

(U) Part of the voting reform implemented under The Help America Vote Act of 2002 was a requirement that the Election Assistance Commission create a set of specifications and requirements against which voting systems can be tested, called the Voluntary Voting System Guidelines (VVSG). The EAC adopted the first VVSG in December 2005. The EAC then tasked the Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST) and including members from NASED, with updating the guidelines. In March 2015, the EAC approved VVSG 1.1; in January 2016, the EAC adopted

[307] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.
[308] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[309] **(U)** *Ibid.*
[310] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[311] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 31.
[312] **(U)** SSCI Transcript of the Interview with Andy McCabe, Deputy Director of the FBI, held on Wednesday, February 14, 2018, pp. 220-221.

an implementation plan requiring that all new voting systems be tested against the VVSG 1.1 beginning in July 2017. VVSG 1.1 has since been succeeded by version 2.0, which was released for a 90-day public comment period on February 15, 2019. The EAC will compile the feedback for Commissioners to review shortly thereafter.[313] VVSG 2.0 includes the following minimum security guidelines:

- **(U)** An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. (9.1)
- **(U)** The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities. (9.2)
- **(U)** Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. (9.3)
- **(U)** The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. (11.3)
- **(U)** The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. (13.1)
- **(U)** The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. (14.2)
- **(U)** The voting system employs mechanisms to protect against malware. (15.3)
- **(U)** A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. (15.4)

(U) As of March 2018, 35 states required that their machines be certified by EAC, but compliance with the VVSG standards is not mandatory. Secretary Nielsen testified before the Committee that the United States should "seek for all states" to use the VVSG standards.[314]

---

[313] **(U)** *EAC Commissioners Unanimously Vote to Publish VVSG 2.0 Principles and Guidelines for Public Comment;* https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/; February 15, 2019

[314] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 47.

VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES

(U) The federal government's actions to address election security threats evolved significantly from the summer of 2016 through the summer of 2018. Contemporaneous with the Russian attacks, DHS and FBI were initially treating the situation as they would a typical notification of a cyber incident to a non-governmental victim. By the fall of 2016, however, DHS was attempting to do more extensive outreach to the states. Then in the fall of 2017, DHS undertook an effort to provide a menu of cyber support options to the states.

A. (U) DHS's Evolution

[redacted] For DHS and other agencies and departments tasked with intelligence collection or formulating policy options through the interagency process, the full scope of the threat began to emerge in the summer of 2016. Secretary Johnson told the Committee that "I know I had significant concerns by [summer of 2016] about doing all we could to ensure the cybersecurity of our election systems."[315] Mr. Daniel said in his interview that by the end of July, the interagency was focused on better protecting electoral infrastructure as part of a "DHS and FBI-led domestic effort."[316]

[redacted] Policymakers quickly realized, however, that DHS was poorly positioned to provide the kind of support states needed. Mr. Daniel said that interagency discussions about the threat "start[ed] a process of us actually realizing that, frankly, we don't actually have very much in the way of capability that we can directly offer the states"—a fact that the states themselves would later echo.[317]

- [redacted] Ms. Monaco said that DHS initially found a "pretty alarming variance in the number of voting registration databases and lack of encryption and lack of backup for all of these things."[318] Ms. Monaco added that "[i]n light of what we were seeing, in light of the intelligence we were getting briefed on, this was a very specific direction and decision to say we need to really accelerate this, put a significant push on resources and engagement at the senior-most levels."[319]

- [redacted] Mr. Daniel and the working group identified DHS's cyber teams as possible assistance to the states. "DHS had teams that could go and provide that support to the private sector. We've been doing that. That's a program that existed for years for critical

---

[315] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[316] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 28.
[317] **(U)** *Ibid.*, p. 38.
[318] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 19.
[319] **(U)** *Ibid.*, p. 21.

infrastructure companies. And we realized that we could repurpose [some of those teams], but we don't have that many of them . . . four or five. It was not very many."[320]

(U) DHS attempted a nuanced outreach to the states on the threat. Ms. Monaco highlighted a delicate balancing act with the interactions with states:

> *I know we tried very hard to strike a balance between engaging state and local officials and federal officials in the importance of raising cyber defenses and raising cybersecurity . . . and not sowing distrust in the system, both because, one, we believed it to be true that the system is in fact quite resilient because of what I mentioned earlier, which is the diffuse nature; and because we did not want to, as we described it, do the Russians' work for them by sowing panic about the vulnerability of the election.*[321]

(U) In an August 15, 2016, conference call with state election officials, then-Secretary Johnson told states, "we're in a sort of a heightened state of alertness; it behooves everyone to do everything you can for your own cybersecurity leading up to the election." He also said that there was "no specific or credible threat known around the election system itself. I do not recall—I don't think, but I do not recall, that we knew about [State 4] and Illinois at that point."[322] The Committee notes that this call was two months after State 4's system was breached, and more than a month after Illinois was breached and the state shut down its systems to contain the problem. During this call, Secretary Johnson also broached the idea of designating election systems as critical infrastructure.

(U) A number of state officials reacted negatively to the call. Secretary Johnson said he was "surprised/disappointed that there was a certain level of pushback from at least those who spoke up. . . . The pushback was: This is our—I'm paraphrasing here: This is our responsibility and there should not be a federal takeover of the election system."[323]

- **(U)** The call "does not go incredibly well," said Mr. Daniel. "I was not on the call, no, but all of the reporting back and then all of the subsequent media reporting that is leaked about the call shows that it did not go well." Mr. Daniel continued: "I was actually quite surprised . . . in my head, there is this: yes, we have this extremely partisan election going on in the background; but the Russians are trying to mess with our election. To me, that's a national security issue that's not dependent on party or anything else."[324]

---

[320] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 41.
[321] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 29.
[322] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 13.
[323] **(U)** *Ibid.*, pp. 13-14.
[324] **(U)** *Ibid.*, p. 48.

- **(U)** Ms. Monaco also related how DHS received significant push back from the states and decided to "focus our efforts on really pushing states to voluntarily accept the assistance that DHS was trying to provide."[325]

- **(U)** States also reported that the call did not go well. Several states told the Committee that the idea of a critical infrastructure designation surprised them and came without context of a particular threat. Some state officials also did not understand what a critical infrastructure designation meant, in practical terms, and whether it would give the federal government the power to run elections. DHS also did not anticipate a certain level of suspicion from the states toward the federal government. As a State 17 official told the Committee, "when someone says 'we're from the government and we're here to help,' it's generally not a good thing."[326]

(U) Critical Infrastructure Designation

(U) One of the most controversial elements of the relationship between DHS and the states was the decision to designate election systems as critical infrastructure. Most state officials relayed that they were surprised by the designation and did not understand what it meant; many also felt DHS was not open to input from the states on whether such a designation was beneficial.

(U) Secretary Johnson remembers the first time he aired the possibility of a designation was on August 3, 2016. He went to a reporters' breakfast sponsored by the Christian Science Monitor and publicly "floated the idea of designating election infrastructure as critical infrastructure."[327] Then, on August 15, 2016, Secretary Johnson had a conference call with election officials from all 50 states. "I explained the nature of what it means to be designated critical infrastructure. It's not a mandatory set of [regulations], it's not a federal takeover, it's not binding operational directives. And here are the advantages: priority in terms of our services and the benefit of the protection of the international cyber norm."[328] Secretary Johnson continued: "I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it."[329]

(U) Some states were vocal in objecting to the idea. In evaluating the states' response, DHS came to the conclusion that it should put the designation on hold, deciding it would earn more state trust and cooperation if it held off on the designation as critical infrastructure and perhaps sought more buy-in from the states at a later date.[330]

---

[325] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 25.
[326] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018.
[327] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[328] **(U)** *Ibid.*, p. 14. For additional information on the definition of critical infrastructure in a cybersecurity context, *see* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[329] **(U)** SSCI Transcript of the Open Hearing on Election Security, March 21, 2018, p. 34.
[330] **(U)** *Ibid.*, p. 115.

(U) After the election, Secretary Johnson decided the time had come to make the designation. He held a follow-up call with NASS on the critical infrastructure designation in January 2017: "I didn't tell them I'm doing this the next day, but I told them I was close to making a decision. I didn't hear anything further [along the lines of additional, articulated objections], so the same day we went public with the [unclassified] version of the report,[331] I also made the designation."[332]

(U) Mr. Daniel summed up the rationale for proceeding this way: "I do believe that we should think of the electoral infrastructure as critical infrastructure, and to me it's just as critical for democracy as communications, electricity, water. If that doesn't function, then your democracy doesn't function. . . . To me that is the definition of 'critical.'"[333]

(U) In interviews with the Committee in late 2017 and early 2018, several states were supportive of the designation and saw the benefits of, for example, the creation of the Government Coordinating Council. Others were lukewarm, saying they had seen limited benefits for all the consternation officials said it had caused. Still others remained suspicious that the designation is a first step toward a federal takeover of elections.

B. (U) The View From the States

(U) For most states, the story of Russian attempts to hack state infrastructure was one of confusion and a lack of information. It began with what states interpreted as an insignificant event: an FBI FLASH notification on August 18, 2016, [redacted][334] Then, in mid-October, the MS-ISAC reached out to state IT directors with an additional alert about specific IP addresses scanning websites.[335] At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor. Given the lack of context, state staff who received the notification did not ascribe any additional urgency to the warning; to them, it was a few more suspect IP addresses among the thousands that were constantly pinging state systems. Very few state IT directors informed state election officials about the alert.

---

[331] **(U)** Secretary Johnson was referring to the declassified version of the Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections,* January 6, 2017.
[332] **(U)** *Ibid.*, p. 46.
[333] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 98.
[334] **(U)** FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[335] **(U)** [redacted] FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

- **(U)** State 11 had a meeting with DHS officials, including the regional DHS cyber advisor, in August 2016, but according to State 11 officials, DHS did not mention any specific threat against election systems from a nation-state actor.[336]

- **(U)** State 13 reported that DHS contacted an affected county at one point, but never contacted the state-level officials.[337]

- **(U)** When they saw an IP address identified in the alerts had scanned their systems, State 6 and State 16 sent their logs to the MS-ISAC for analysis.[338] State 16 said it never received a response.[339]

(U) DHS, conversely, saw its efforts as far more extensive and effective. Ms. Manfra testified to SSCI that DHS "held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility [participated], in August, in September, and again in October [of 2016], both high-level engagement and network defense products [sic]."[340] Mr. Daniel reported that "by the time Election Day rolls around, all but one state has taken us up on the offer to at least do scanning [,] so I want to give people credit for not necessarily sticking to initial partisan reactions and . . . taking steps to protect their electoral infrastructure."[341]

(U) States reported to the Committee that Election Day went off smoothly. For most state election officials, concerns about a possible threat against election systems dropped off the radar until the summer or fall of 2017. Many state election officials reported hearing for the first time that Russian actors were responsible for scanning election infrastructure in an estimated 21 states from the press or from the Committee's open hearing on June 21, 2017. During that hearing, in response to a question from Vice Chairman Warner inquiring whether all affected states were aware they were attacked, Ms. Manfra responded that "[a]ll of the system owners within those states are aware of the targeting, yes, sir."[342] However, when pressed as to whether election officials in each state were aware, the answer was less clear.[343]

- **(U)** In that hearing, Dr. Liles said DHS had "worked hand-in-hand with the state and local partners to share threat information related to their networks."[344]

---

[336] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[337] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[338] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[339] **(U)** *Ibid.* State 6 did not indicate whether they received feedback from DHS.
[340] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, June 21, 2017, p. 74.
[341] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 49.
[342] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 28.
[343] **(U)** *Ibid.*, pp. 62-63.
[344] **(U)** *Ibid.*, p. 12.

- (U) Ms. Manfra said, "The owners of the systems within those 21 states have been notified." Senator King then asked, "How about the election officials in those states?" Ms. Manfra responded, "We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states ....[crosstalk]."[345]

- (U) Given Ms. Manfra's testimony and the fact that some election officials did not get a notification directly to their offices, election officials in many states assumed they were not one of the 21; some even issued press releases to that effect.[346]

(U) The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was any different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials.

(U) After the hearing, and in part to respond to confusion in the states, DHS held a conference call with representatives from 50 states in September 2017. In that call, DHS said they would contact affected states directly. State 8 state election officials noted that the call became "somewhat antagonistic."[347] State 17 officials reported that the phone call "just showed how little DHS knew about elections."[348] Several officials argued that all 50 states should be notified of who had been hacked. DHS followed up with one-to-one phone calls to states over the next several days.

- (U) Officials from some states reported being shocked that they were in fact one of the states, and further surprised that their states had supposedly been notified.

- (U) Most state officials found the conference calls lacking in information and were left wondering exactly what the threat might be. Several states said the DHS representatives could not answer any specific questions effectively.

(U) Following this series of difficult engagements, DHS set about trying to build relationships with the states, but it faced a significant trust deficit. Early follow-up interactions between state election officials and DHS were rocky. States reported that DHS seemed to have little to no familiarity with elections. For example, State 6 said that the DHS representatives they were assigned seemed to know nothing about State 6, and, when pressed, they admitted they were "just reading the spreadsheet in front of [them]."[349] State 8 reported that "we are spending

---

[345] (U) *Ibid.*, pp. 62-63.
[346] (U) State 8 said they put out a press release because DHS had said publicly that they had notified the 21 states, and "if you were one of the 21, you would know."
[347] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[348] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[349] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

a ton of time educating outside groups on how elections are run."[350] State 3 officials said, "DHS didn't recognize that securing an election process is not the same as securing a power grid."[351]

(U) By early 2018, State officials gave DHS credit for making significant progress over the next six months. States began to sign up for many of the resources that DHS had to offer, and DHS hosted the first meeting of the Government Coordinating Council required under the critical infrastructure designation. Those interactions often increased trust and communication between the federal and state entities. For example, DHS has identified a list of contacts to notify if they see a threat; that list includes both IT officials and election officials. State 9 described it as "quite a turnaround for DHS," and further stated that the Secretaries of State had been disappointed with how slowly DHS got up to speed on election administration and how slowly the notifications happened, but DHS was "quick with the *mea culpas* and are getting much better." [352]

(U) Not all of the engagements were positive, however. State 13 in early December 2017 still reported continued frustration with DHS, indicating to the Committee that it had not seen much change in terms of outreach and constructive engagement. As of summer 2017, according to State 13, "the lack of urgency [at DHS] was beyond frustrating."[353]

C. (U) Taking Advantage of DHS Resources

(U) As DHS has pursued outreach to the states, more and more have opened their doors to DHS assistance. DHS told the Committee that its goal has been relationship building and:

> *In the partnerships with the states and secretaries of states, state election directors, and at the local level, we're trying to shift them to a culture of more information security management, where they can now account for the integrity of their system, or, if something did happen . . . they know the full extent of what happened on their system. . . . We're providing vulnerability assessments and trend analysis, in addition to connecting them to the threat intelligence that we can, in order to evolve their . . . cyber culture.* [354]

(U) DHS's assistance can be highly tailored to need, and falls into roughly two buckets: remote cyber hygiene scans, which provide up to weekly reports, and on-site risk and vulnerability assessments. DHS also offers a suite of other services, including phishing campaign assessments. All these efforts seek to provide the states with actionable information to improve cyber hygiene, but DHS has been keen to avoid what could be perceived by the states as

---

[350] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[351] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.
[352] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[353] (U) Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[354] (U) SSCI interview with DHS and CTIIC, February 27, 2018, pp. 54-55.

unfunded mandates.[355] Some states requesting more intensive services have also experienced significant delays before DHS could send a team to assist.

- **(U)** By October 2018, DHS said 35 states, 91 local jurisdictions, and eight election system vendors had signed up for remote persistent scans.[356] All the requests for these scans have been fulfilled. "They can be turned on basically within the week," according to DHS.[357]

- **(U)** DHS said that as of October 2018, it had completed 35 in-depth, on the ground vulnerability assessments: 21 states, 13 localities, and one election system vendor. These assessments are one week off-site remote scans followed by a second week on site.[358]

- **(U)** Two states who completed the in-depth assessments reported in late 2017 they had had a good experience. State 12 officials said the team was "extremely helpful and professional."[359] State 10 said the review was a good experience, although DHS was somewhat limited in what it could do.[360] For example, DHS did a phishing email test that showed the training for employees had worked.[361] DHS gave "good and actionable recommendations." Although DHS "didn't really understand election systems when they came," they learned a lot.[362]

- **(U)** As of November 2017, State 6 and State 9 requested an on-site scan, but those scans were on track to be delayed past the August 2018 primaries.[363] State 7 was expecting a four-to-six month delay.[364] State 8 signed up for a checkup in October 2017 and was due to get service the following February.[365] As of January 2018, State 17 also had requested an on-site scan.[366]

(U) In a sign of improving relations between the states and DHS, two states that had elections in 2017 attempted to include DHS in the process more extensively than in the past. In State 17, a two-person DHS team sat with election officials during the 2017 special election and monitored the networks. Even though "their presence was comforting," they "really didn't do much." State 17 signed DHS's normal MOU, but also added its own clause to underscore the state's independence: a formal sunset on DHS's access to state systems, one week after the

---

[355] **(U)** *Ibid.*, p. 60.
[356] **(U)** *Ibid.*, p. 57.
[357] **(U)** DHS phone call with SSCI: October 16, 2018.
[358] **(U)** *Ibid.*
[359] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[360] **(U)** *Ibid.*
[361] **(U)** *Ibid.*
[362] **(U)** *Ibid.*
[363] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[364] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[365] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[366] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

election. State 7 reported their experience with DHS during the 2017 statewide election was quite good. DHS sat with election officials all day, which meant State 7 could pass messages quickly to NCCIC.

(U) In March 2018, Congress appropriated $380 million in funding for election security improvements. The funding was distributed under the formula laid out in the Help American Vote Act (HAVA) and was intended to aid in replacing vulnerable voting machines and improving cybersecurity. As of July 2018, 13 states said they intended to use the funds to buy new voting machines, and 22 said they have "no plans to replace their machines before the election—including all five states that rely solely on paperless electronic voting devices," according to a survey by Politico.[367]

IX. (U) RECOMMENDATIONS

1. (U) Reinforce States' Primacy in Running Elections*

(U) States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.

2. (U) Build a Stronger Defense, Part I: Create Effective Deterrence

(U) The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

[redacted] **Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government.** That doctrine should clearly delineate cyberespionage, cybercrime, and cyber attacks. Further, a classified portion of the doctrine should establish what the U.S. Government believes to be its escalation ladder in the cyber realm—what tools does it have, what tools should it pursue, and what should the limits of cyber war be. The U.S. strategic approach tends to overmatch adversaries with superior technology, and policymakers should consider what steps the U.S. will need to take to outstrip the capabilities of Russia, China, Iran, North Korea, and other emerging hostile actors in the cyber domain.

(U) U.S. cyber doctrine should serve as the basis for a discussion with U.S. allies and others about new cyber norms. Just as the international community has established norms and treaties about the use of technologies and weapons systems, the U.S. should lead a conversation about cyber norms and the limits of cyber activity with allies and others.

*The Committee's recommendation to "reinforce states' primacy in running elections" should be understood in reference to states' responsibility for election security, and not as pertaining to broader election issues, such as campaign finance laws or voting rights laws.

[367] (U) States Slow to Prepare for Hacking Threats, Eric Geller, Politico, July 18, 2018.

3. (U) Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats

[redacted]

[redacted] **The U.S. government needs to build the cyber expertise and capacity of its domestic agencies, such as DHS and FBI, and reevaluate the current authorities that govern efforts to defend against foreign cyber threats.** NSA and CIA collection is, by law, directed outside the United States. [redacted]

[redacted] **The U.S. government should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy.** [redacted] However, the IC needs to improve its ability to provide timely and actionable warning. Timely and accurate attribution is not only important to defensive information sharing, but will also underpin a credible deterrence and response strategy.

(U) **The federal government and state governments need to create clear channels of communication two ways—down from the federal government to the state and local level, and up from the state and local officials on the front lines to federal entities**. In 2016, DHS and FBI did not provide enough information or context to election officials about the threat they were facing, but states and DHS have made significant progress in this area in the last two years. For example, Secretary of Homeland Security Nielsen testified to the Committee in March 2018 that "today I can say with confidence that we know whom to contact in every state to share threat information. That capability did not exist in 2016."[369]

(U) **A key component of information sharing about elections is security clearances for appropriate officials at the state and local level.** DHS and its partners can effectively strip classified information off of cyber indicators, which can then be passed to technical staff at the state level, but in order for those indicators to not get lost in the multitude of cyber threats those professionals see on a daily basis, senior officials at the state and local levels need to know the

---

[368] [redacted]

[369] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 16.

context surrounding the indicators. State officials need to know why a particular threat is of significant concern, and should be prioritized. That context could come from classified information, or states could come to understand that threat information DHS passes them is more serious than that received through other sources. DHS's goal is to obtain clearances for up to three officials per state.[370] As of August 2018, DHS had provided a clearance to 92 officials[371]; as of late 2017 all state election officials had received interim secret clearances or one-day read-ins for secret-level briefings.[372] DHS, along with ODNI and FBI, also hosted state and local election officials for a SECRET-level briefing on the sidelines of the biannual NASS and NASS-ED conferences in Washington, DC in February 2018. In March, Amy Cohen, Executive Director of NASS-ED testified in front of the Committee that, "It would be naïve to say that we received answers to all our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns."[373] The Committee recommends DHS continue providing such briefings and improve the quality of information shared.

(U) Fundamental to meaningful information sharing, however, is that state officials understand what they are getting. New inductees to the world of classified information are often disappointed—they expected to see everything laid out in black and white, when intelligence is often very gray, with a pattern discernable only to those who know where to look and what conclusions to draw. Those sharing the intelligence should manage expectations—at the SECRET level, officials are likely to see limited context about conclusions, but not much more.

(U) Federal officials should work to declassify information, for the purpose of providing warning to appropriate state and local officials, to the greatest extent possible. If key pieces of context could be provided at a lower classification level while still protecting classified information, DHS and its partners should strive to do so.

4. (U) Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems

(U) Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help.

(U) The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities. The Committee additionally recommends that State officials:

---

[370] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.15.
[371] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[372] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p 15, 26.
[373] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.113.

- **(U)** Identify the weak points in their networks, like under-resourced localities. State 7 said they are not worried about locations like larger counties when it comes to network security, but they are worried about "the part-time registrar who is also the town attorney and the town accountant and is working out of a 17th century jail." [374]

- **(U)** Undertake security audits of state and local voter registration systems, ideally utilizing private sector entities capable of providing such assistance. State and local officials should pay particular attention to the presence of high severity vulnerabilities in relevant web applications, as well as highly exploitable vulnerabilities such as cross-site scripting and SQL injection.

- **(U)** Institute two-factor authentication for user access to state databases.

- **(U)** Install monitoring sensors on state systems. As of mid-2018, DHS's ALBERT sensors covered up to 98% of voting infrastructure nationwide, according to Undersecretary Krebs.[375]

- **(U)** Include voter registration database recovery in state continuity of operations plans.

- **(U)** Update software in voter registration systems. One state mentioned that its voter registration system is more than ten years old, and its employees will "start to look for shortcuts" as it gets older and slower, further imperiling cybersecurity.

- **(U)** Create backups, including paper copies, of state voter registration databases.

- **(U)** Consider a voter education program to ensure voters check registration information well prior to an election.

(U) DHS in the past year has stepped up its ability to assist the states with some of these activities, but DHS needs to continue its focus on election infrastructure and pushing resources to the states.

(U) The Committee recommends DHS take the following steps:

- **(U)** Create an advisory panel to give DHS expert-level advice on how states and localities run elections. The Government Coordinating Council, created as part of the critical infrastructure designation, could serve as a venue for educating DHS on what states do and what they need.

---

[374] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[375] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- **(U)** Create guidelines on cybersecurity best practices for elections and a public awareness campaign to promote election security awareness, working through EAC, NASS, and NASED, and with the advisory panel.

- **(U)** Develop procedures and processes to evaluate and routinely provide guidance on relevant vulnerabilities associated with voting systems in conjunction with election experts.

- **(U)** DHS has already created a catalog of services they can provide to states to help secure states' systems. DHS should maintain the catalog and continue to update it as it refines its understanding of what states need.

- **(U)** Expand capacity so wait times for services, like voluntary vulnerability assessments, are manageable and so that DHS can maintain coverage on other critical infrastructure sectors. Robbing resources from other critical infrastructure sectors will eventually create unacceptable new vulnerabilities.

- **(U)** Work with GSA to establish a list of approved private-sector vendors who can provide services similar to those DHS provides. States report being concerned about "vultures" —companies who show up selling dubious cyber solutions. That being said, some states will be more comfortable having a private sector entity evaluate their state systems than a federal agency.

- **(U)** Continue to build the resources of the newly established EI-ISAC. States have already found this information sharing service useful, and it could serve as a clearinghouse for urgent threat information. As of August 2018, the EI-ISAC had over 1,000 members with participants in all 50 states.[376]

- **(U)** Continue training for state and local officials, like the table-top exercise conducted in August of 2018 that brought together representatives from 44 states, localities, and the federal government to work through an election security crisis.[377] The complexity of the scenario encouraged state and local officials to identify serious gaps in their preparations for Election Day.

5. (U) Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself

(U) Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

---

[376] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[377] **(U)** DHS, Press release: DHS Hosts National Exercise on Election Security, August 15, 2018.

- (U) As states look to replace HAVA-era machines that are now out of date, they should purchase more secure voting machines. Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability.

- (U) States should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. State purchasers should write contracts with vendors to ensure adherence to the highest security standards and to demand guarantees the supply chains for machines are secure.

- (U) In concert with the need for paper ballots comes the need to secure the chain of custody for those ballots. States should reexamine their safeguards against insertion of fraudulent paper ballots at the local level, for example time stamping when ballots are scanned.

- (U) Statistically sound audits may be the simplest and most direct way to ensure confidence in the integrity of the vote.[378] States should begin to implement audits of election results. Logic and accuracy tests of machines are a common step, but do not speak to the integrity of the actual vote counting. Risk-limiting audits, or some similarly rigorous alternative, are the future of ensuring that votes cast are votes counted. State 8, State 12, State 21, State 9, State 2, State 16, and others already audit their results, and others are exploring additional pilot programs.[379] However, as of August 2018, five states conducted no post-election audit and 14 states do not do a complete post-election audit.[380] The Committee recognizes states' concern about the potential cost of such audits and the necessary changes to state laws and procedures; however, the Committee believes the benefit of having a provably accurate vote is worth the cost.

- (U) States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members

---

[378] (U) Election experts point out, however, that audits could create a new vector for election-related lawsuits. Complainants could allege that the audit was done improperly, or that the audit process reflected bias.

[379] (U) State 8 passed a law to audit starting in 2018, with random precinct sampling. State 12 does state-wide audits. State 21 audits 2% of ballots, randomly selected. State 9 picks 210 of 4100 precincts at random for an audit. State 2 hand-counts ballots in randomly selected precincts and uses automated software to test. A States law on ballot storage can't accommodate risk-limiting audits. Instead, they use ClearBallot software. They upload images of ballots to an external hard drive and send it to ClearBallot. ClearBallot is blind to who won and independently evaluates the results. In addition, the company can identify problems with scanners; for example, when a fold in absentee ballots recorded as a vote. Cybersecurity experts still doubt, however, that this type of procedure is secure.

[380] (U) DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

of the military get to vote for their elected officials, no system of online voting has yet established itself as secure.[381]

- **(U)** DHS should work with vendors of election equipment to educate them about the vulnerabilities in both the machines and the supply chains for the components of their machines. Idaho National Lab is already doing some independent work on the security of a select set of voting machines, developing a repeatable methodology for independently testing the security of such systems.

- **(U)** The Department of State should work with FBI and DHS to warn states about foreign efforts to access polling places outside normal channels in the future and remain vigilant about rejecting aberrant attempts.

- **(U)** The Associated Press is responsible for reporting unofficial, initial election results on election night and is a critical part of public confidence in the voting tally. States and DHS should work with the AP and other reporting entities to ensure they are both secure and reporting accurate results.

- **(U)** The Committee found that, often, election experts, national security experts, and cybersecurity experts are speaking different languages. Election officials focus on transparent processes and open access and are concerned about introducing uncertainty into the system; national security professionals tend to see the threat first. Both sides need to listen to each other better and to use more precise language.

6. (U) Assistance for the States

(U) State officials told the Committee the main obstacle to improving cybersecurity and purchasing more secure voting machines is cost. State budgets are stretched thin by priorities that seem more urgent on a daily basis and are far more visible to constituents.

(U) In March 2018, Congress appropriated $380 million in funds under the HAVA formula for the states. As of August 2018, states had begun to allocate and spend that money for items such as cybersecurity improvements.

(U) The Committee recommends the EAC, which administers the grants, regularly report to Congress on how the states are using those funds, whether more funds are needed, and whether states have both replaced outdated voting equipment and improved

---

[381] **(U)** Dr. Halderman in his testimony before the Committee said, "I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence. And I say that having myself . . . hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use." *See* SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 152.

cybersecurity. More funds may be needed, as the allocation under the HAVA formula did not prioritize replacing vulnerable electronic-only machines.

- **(U)** States should be able to use grant funds to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting with vendors to provide cybersecurity services. "Security training funded and provided by a federal entity such as the EAC or DHS would also be beneficial in our view,"[382] an official from Illinois testified.

- **(U)** Funds should also be available to defray the cost of instituting audits.

- **(U)** States with vulnerable DRE machines with no paper backup should receive urgent access to funding. Dr. Halderman testified that replacing insecure paperless voting machines nationwide would cost $130 to $400 million dollars. Risk-limiting audits would cost less than $20 million a year.[383]

7. [redacted] **Build a Credible** [redacted]

[redacted]

[382] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 114.
[383] **(U)** *Ibid.*, p. 119.

MINORITY VIEWS OF SENATOR WYDEN

(U) The role of the federal government

(U) The Committee report describes Russian attacks on U.S. election infrastructure in 2016 and lays out many of the serious vulnerabilities that exist to this day. These vulnerabilities pose a direct and urgent threat to American democracy which demands immediate congressional action. The defense of U.S. national security against a highly sophisticated foreign government cannot be left to state and county officials. For that reason, I cannot support a report whose top recommendation is to "reinforce[ ] state's primacy in running elections."

(U) Congress's constitutional role in regulating federal elections is well-established. In response to an inquiry from the bipartisan leadership of the U.S. Senate, the General Accounting Office (GAO) wrote that "[w]ith regard to the administration of federal elections, Congress has constitutional authority over both congressional and presidential elections."[1] Indeed, pursuant to the Elections Clause of the U.S. Constitution,[2] Congress's authority over congressional elections is "paramount to that of the states." As the GAO report details, Congress has repeatedly passed legislation related to the administration of elections on topics such as the timing of federal elections, voter registration, absentee voting requirements, disability access, and voting rights.

(U) If there was ever a moment when Congress needed to exercise its clear constitutional authorities to regulate elections, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again. The federal government's response to this ongoing crisis cannot be limited offers to provide resources and information, the acceptance of which is voluntary. If the country's elections are to be defended, Congress must also establish mandatory, nation-wide cybersecurity requirements.

(U) Security of voting machines

(U) Experts are clear about the measures necessary to protect U.S. elections from cyber manipulation.[3] Absent an accessibility need, most voters should hand-mark paper ballots. For voters with some kind of need, ballot marking devices that print paper ballots should be available. Risk-limiting audits must be also be required. Currently, however, only Virginia, Colorado and Rhode Island meet these requirements.[4] These critical reforms must be adopted

---

[1] "Elections. The Scope of Congressional Authority in Election Administration," General Accounting Office, March 2001, prepared in response to a joint inquiry from Senator Trent Lott, Republican Leader; Senator Tom Daschle, Democratic Leader; Senator Mitch McConnell, Chairman, and Senator Christopher Dodd, Ranking Member, of the Senate Committee on Rules and Administration.

[2] Article I, Section 4, Clause 1

[3] Securing the Vote; Protecting American Democracy; National Academy of Sciences, Engineering and Medicine, September 2018

[4] National Conference of State Legislatures, Post-Election Audits, January 3, 2019. Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018. Oregon requires paper ballots and the Oregon State Senate has passed a bill requiring risk-limiting audits.

throughout the country, which is why, on June 27, 2019, the House of Representatives passed H.R. 2722, the Securing America's Federal Elections (SAFE) Act. The security of the country's voting machines depends on this legislation being signed into law.

(U) The Committee, in recommending basic security measures like paper ballots and audits, notes that there is currently "a wide range of cybersecurity practices across the states." Indeed, the data is deeply concerning and highlights the need for mandatory, nation-wide standards. For example, the Committee rightly highlights the vulnerabilities of Direct-Recording Electronic (DRE) Voting Machines, noting that, without a paper trail, there would be no way to conduct a meaningful "recount" and compromises would remain undetected. As of November 2018, however, there were still four states in which every single county relied on DREs without voter verified paper audit trail printers (VVPAT) and, in an additional eight states, there were multiple counties that relied on DREs without a VVPAT.[5] Gaps in the deployment of VVPATs, which are far less secure than hand-marked paper ballots, demonstrate that even bare minimum security best practices are not being met in many parts of the country.

(U) In addition, 16 states have no post-election audits of any kind, while many others have insufficient or perfunctory audits. Only four states have a statutory requirement for risk-limiting audits, while two states provide options for counties to run different kinds of audits, one of which is a risk-limiting audit.[6] Next year, a third state will provide that option. In other words, the vast majority of states have made no moves whatsoever toward implementing minimum standards that experts agree are necessary to guarantee the integrity of elections.

(U) The Committee rightly identifies problems with vendors of voting machines, noting vulnerabilities in both the machines and the supply chains for machine components. Currently, however, the federal government has no regulatory authority that would require these vendors to adhere to basic security practices.[7] Only general federal requirements that states and localities use paper ballots and conduct audits will ensure that the risk posed by voting machines provided by private vendors to states and localities can be contained. The stakes could not be more clear. As Homeland Secretary Kirstjen Nielsen testified to the Committee, "If there is no way to audit the election, that is absolutely a national security concern."[8]

(U) Registration databases and election night reporting websites

(U) Two additional components of the U.S. election infrastructure require immediate, mandatory cybersecurity fixes. The first are voter registration databases. The Committee received testimony about successful Russian exfiltration of databases of tens of thousands of voters.[9] Expert witnesses also described the chaos that manipulated voter registration data could cause should voters arrive at the polls and find that their names had been removed from the rolls.

---

[5] Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018.
[6] The four states are Colorado, Nevada, Rhode Island, and Virginia. National Conference of State Legislatures, Post-Election Audits, January 3, 2019.
[7] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[8] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.
[9] Testimony of Connie Lawson, President-elect, National Association of Secretaries of State, and Secretary of State, State of Indiana; testimony of Steve Sandvoss, Executive Director of Illinois State Board of Elections, June 21, 2017; Illinois Voter Registration System Database Breach Report.

As one expert testified, this form of interference "could be used to sabotage the election process on Election Day."[10]

(U) The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require states to implement even minimum cybersecurity measures. There are not even any voluntary federal standards.

(U) An additional component of the U.S. election infrastructure that requires immediate, mandatory cybersecurity measures are the election night reporting websites run by the states. The Committee heard testimony about a Russian attack on Ukraine's web page for announcing results. That attacked allowed the Russians to use misinformation that left Ukraine in chaos for days after the election. As the Committee's expert witness warned, "[w]e need to look at that playbook. They will do it to us."[11] Like voter registration databases, election results websites are not subject to any mandatory standards. Both of these critical vulnerabilities, as well as vulnerabilities of voting machines, must be addressed by the U.S. Congress through the passage of S. 2238, the Senate version of the SAFE Act.

(U) Given the inconsistent, and at times non-existent adherence to basic cybersecurity among states and localities, I cannot agree with the Committee's conclusion that "the country's decentralized election system can be a strength from a cybersecurity perspective." Until election security measures are required of every state and locality, there will be vulnerabilities to be exploited by our adversaries. The persistence of those vulnerabilities has national consequences. The manipulation of votes or voter registration databases in any county in the country can change the result of a national election. The security of the U.S. election system thus hinges on its weakest links – the least capable, least resourced local election offices in the country, many of which do not have a single full-time employee focused on cybersecurity.

(U) Every American has a direct stake in the cybersecurity of elections throughout the country. Congress has an obligation to protect the country's election system everywhere. If there were gaps in the defense of our coastline or air space, members would ensure that the federal government close them. Vulnerabilities in the country's election cybersecurity require the same level of national commitment.

(U) Cybersecurity vulnerabilities and influence campaigns

(U) The cybersecurity vulnerabilities of the U.S. election system cannot be separated from Russia's efforts to influence American voters. As the January 2017 Intelligence Community Assessment (ICA) concluded, and as the Committee report notes, the Russians were "prepared to publicly call into question the validity of the results" and "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory." This plan highlights an additional reason why nation-wide election cybersecurity standards are so critical. If Russia's preferred candidate does not prevail in the 2020 election, the

---

[10] Testimony of Alex J. Halderman, Professor of Computer Science and Engineering, University of Michigan, June 21, 2017.

[11] Testimony of Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs, Harvard Kennedy School, March 21, 2018.

Russians may seek to delegitimize the election. The absence of any successful cyber intrusions, exfiltrations or manipulations would greatly benefit the U.S. public in resisting such a campaign.

(U) While not formally part of the U.S. election infrastructure, the devices and accounts of candidates and political parties represent an alarming vulnerability in the country's overall election system. Russia's campaign of hacking the emails of prominent political figures and releasing them through Wikileaks, Gucifer 2.0, and DCLeaks was probably its most effective means of influencing the 2016 election. The Committee has received extensive testimony about these operations, the vulnerabilities that allowed them to occur, and the threat those vulnerabilities pose to the integrity of American democracy.[12] Yet little has been done to prevent it from happening all over again. S. 1569, the Federal Campaign Cybersecurity Assistance Act of 2019, addresses these vulnerabilities head on by authorizing political committees to provide cybersecurity assistance to candidates, campaigns and state parties.

(U) These vulnerabilities extend to the U.S. Senate, most of whose members are or will be candidates for reelection or for other positions. As a November 2018 Senate report noted, there is "mounting evidence that Senators are being targeted for hacking, which could include exposure of personal data."[13] Private communications and information reside on personal accounts and devices. Passage of S. 890, the Senate Cybersecurity Protection Act, will authorize the Senate Sergeant at Arms to protect the personal devices and accounts of Senators and their staff and help prevent the weaponization of their data in campaigns to influence elections.

(U) Assessments related to the 2016 election

(U) I have also submitted these Minority Views to address assessments related to Russian activities during the 2016 election. According to the January 2017 ICA, DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." An assessment based on observations is only as good as those observations and this assessment, in which DHS had only moderate confidence,[14] suffered from a lack of observable data. As Acting Deputy Undersecretary of Homeland Security for National Protection and Programs Directorate, Jeannette Manfra, testified at the Committee's June 21, 2017, hearing, DHS did not conduct any forensic analysis of voting machines.

(U) DHS's prepared testimony at that hearing included the statement that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected." The language of this assessment raises questions, however, about DHS's ability to identify cyber manipulation that could have affected a very close national election, particularly given DHS's acknowledgment of the "possibility that individual or isolated cyber

---

[12] See, for example, Committee hearing, March 30, 2017.

[13] Senators' Personal Cybersecurity Working Group Report, submitted by the Senators' Personal Cybersecurity Working Group, November 2018.

[14] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following Committee hearing, June 21, 2017.

intrusions into U.S. election infrastructure could go undetected, especially at local levels."[15] Moreover, DHS has acknowledged that its assessment with regard to the detection of outcome-changing cyber manipulation did not apply to state-wide or local elections.[16]

(U) Assessments about manipulations of voter registration databases are equally hampered by the absence of data. As the Committee acknowledges, it "has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases." Assessments about Russian attacks on the administration of elections are also complicated by newly public information about the infiltration of an election technology company. Moreover, as the Special Counsel reported, the GRU sent spear phishing emails to "Florida county officials responsible for administering the 2016 election" which "enabled the GRU to gain access to the network of at least one Florida county government."[17]

(U) The Committee, in stating that it had found no evidence that vote tallies were altered or that voter registry files were deleted or modified, rightly noted that the Committee's and the IC's insight into this aspect of the 2016 election was limited. I believe that the lack of relevant data precludes attributing any significant weight to the Committee's finding in this area.

(U) The Committee's investigation into other aspects of Russia's interference in the 2016 election will be included in subsequent chapters. I look forward to reviewing those chapters and hope that outstanding concerns about members' Committee staff access to investigative material, including non-compartmented and unclassified information, will be resolved.

[15] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[16] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[17] Report on the Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller III, March 2019

ADDITIONAL VIEWS OF SENATORS HARRIS, BENNET, AND HEINRICH

(U) The Russian government's attack on the 2016 election was the product of a deliberate, sustained, and sophisticated campaign to undermine American democracy. Russian military intelligence carried out a hacking operation targeting American political figures and institutions. The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate. And, as this report makes clear, individuals affiliated with the Russian government launched cyber operations that attempted to access our nation's election infrastructure, in some cases succeeding.

(U) The Russian objectives were clear: deepen distrust in our political leaders; exploit and widen divisions within American society; undermine confidence in the integrity of our elections; and, ultimately, weaken America's democratic institutions and damage our nation's standing in the world. The Committee did not discover evidence that Russia changed or manipulated vote tallies or voter registration information, however Russian operatives undoubtedly gained familiarity with our election systems and voter registration infrastructure—valuable intelligence that it may seek to exploit in the future.

(U) The Committee's report does not merely document the wide reach of the Russian operation; the report reveals vulnerabilities in our election infrastructure that we must collectively address. We do not endorse every recommendation in the Committee's report, and we share some of our colleagues' concerns about the vulnerability that we face, particularly at the state level, where counties with limited resources must defend themselves against sophisticated nation-state adversaries. Nevertheless, the report as a whole makes an important contribution to the public's understanding of how Russia interfered in 2016, and underscores the importance of working together to defend against the threat going forward.

(U) It is critical that state and local policymakers study the report's findings and work to secure election systems by prioritizing cybersecurity, replacing outdated systems and machines, and implementing audits to identify and limit risk. The Intelligence Community and other federal agencies must improve efforts to detect cyberattacks, enhance coordination with state and local officials, and develop strategies to mitigate threats. And, critically, Congress must take up and pass legislation to secure our elections. We must provide states the funding necessary to modernize and maintain election infrastructure, and we must take commonsense steps to safeguard the integrity of the vote, such as requiring paper ballots in all federal elections.

(U) Our adversaries will persist in their efforts to undermine our shared democratic values. In order to ensure that our democracy endures, it is imperative that we recognize the threat and make the investments necessary to withstand the next attack.

Allied Security Operations Group

Antrim Michigan Forensics Report

REVISED PRELIMINARY SUMMARY, v2

Report Date 12/13/2020

Client: **Bill Bailey**

Attorney: **Matthew DePerno**

A. WHO WE ARE

1. My name is Russell James Ramsland, Jr., and I am a resident of Dallas County, Texas. I hold an MBA from Harvard University, and a political science degree from Duke University. I have worked with the National Aeronautics and Space Administration (NASA) and the Massachusetts Institute of Technology (MIT), among other organizations, and have run businesses all over the world, many of which are highly technical in nature. I have served on technical government panels.

2. I am part of the management team of Allied Security Operations Group, LLC, (ASOG). ASOG is a group of globally engaged professionals who come from various disciplines to include Department of Defense, Secret Service, Department of Homeland Security, and the Central Intelligence Agency. It provides a range of security services, but has a particular emphasis on cybersecurity, open source investigation and penetration testing of networks. We employ a wide variety of cyber and cyber forensic analysts. We have patents pending in a variety of applications from novel network security applications to SCADA (Supervisory Control and Data Acquisition) protection and safe browsing solutions for the dark and deep web. For this report, I have relied on these experts and resources.

B. PURPOSE AND PRELIMINARY CONCLUSIONS

1. The purpose of this forensic audit is to test the integrity of Dominion Voting System in how it performed in Antrim County, Michigan for the 2020 election.

2. We conclude 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 electronic ballots are then transferred for adjudication. 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. Based on our study, we conclude that The Dominion Voting System should not be used in Michigan. We further conclude that the results of Antrim County should not have been certified.

3. The following is a breakdown of the votes tabulated for the 2020 election in Antrim County, showing different dates for the tabulation of the same votes.

Date	Registered Voters	Total Votes Cast	Biden	Trump	Third Party	Write-In	TOTAL VOTES for President
Nov 3	22,082	16,047	7,769	4,509	145	14	12,423
Nov 5	22,082	18,059	7,289	9,783	255	20	17,327
Nov 21	22,082	16,044	5,960	9,748	241	23	15,949

4. The Antrim County Clerk and Secretary of State Jocelyn Benson have stated that the election night error (detailed above by the vote "flip" from Trump to Biden, was the result of human error caused by the failure to update the Mancelona Township tabulator prior to election night for a down ballot race. We disagree and conclude that the vote flip occurred because of machine error built into the voting software designed to create error.

5. Secretary of State Jocelyn Benson's statement on November 6, 2020 that "[t]the correct results always were and continue to be reflected on the tabulator totals tape . . . ." was false.

6. The allowable election error rate established by the Federal Election Commission guidelines is of 1 in 250,000 ballots (.0008%). We observed an error rate of 68.05%. This demonstrated a significant and fatal error in security and election integrity.

7. The results of the Antrim County 2020 election are not certifiable. This is a result of machine and/or software error, not human error.

8. The tabulation log for the forensic examination of the server for Antrim County from December 6, 2020consists of 15,676 individual events, of which 10,667 or 68.05% of the events were recorded errors. These errors resulted in overall tabulation errors or ballots being sent to adjudication. This high error rates proves the Dominion Voting System is flawed and does not meet state or federal election laws.

9. These errors occurred after The Antrim County Clerk provided a re-provisioned CF card with uploaded software for the Central Lake Precinct on November 6, 2020. This means the statement by Secretary Benson was false. The Dominion Voting System produced systemic errors and high error rates both prior to the update and after the update; meaning the update (or lack of update) is not the cause of errors.

10. In Central Lake Township there were 1,222 ballots **reversed** out of 1,491 total ballots cast, resulting in an 81.96% rejection rate. All reversed ballots are sent to adjudication for a decision by election personnel.

11. It is critical to understand that the Dominion system classifies ballots into two categories, 1) normal ballots and 2) adjudicated ballots. Ballots sent to adjudication can be altered by administrators, and adjudication files can be moved between different Results Tally and Reporting (RTR) terminals with no audit trail of which administrator actually adjudicates (i.e. votes) the ballot batch. This demonstrated a significant and fatal error in security and election integrity because it provides no meaningful observation of the adjudication process or audit trail of which administrator actually adjudicated the ballots.

12. A staggering number of votes required adjudication. This was a 2020 issue not seen in previous election cycles still stored on the server. This is caused by intentional errors in the system. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency or audit trail. Our examination of the server logs indicates that this high error rate was incongruent with patterns from previous years. The statement attributing these issues to human error is not consistent with the forensic evaluation, which points more correctly to systemic machine and/or software errors. The systemic errors are intentionally designed to create errors in order to push a high volume of ballots to bulk adjudication.

13. The linked video demonstrates how to cheat at adjudication:

    https://mobile.twitter.com/KanekoaTheGreat/status/1336888454538428418

14. Antrim County failed to properly update its system. A purposeful lack of providing basic computer security updates in the system software and hardware demonstrates incompetence, gross negligence, bad faith, and/or willful non-compliance in providing the fundamental system security required by federal and state law. There is no way this election management system could have passed tests or have been legally certified to conduct the 2020 elections in Michigan under the current laws. According to the National Conference of State Legislatures – Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.

15. Significantly, the computer system shows vote adjudication logs for prior years; but all adjudication log entries for the 2020 election cycle are missing. The adjudication process is the simplest way to manually manipulate votes. The lack of records prevents any form of audit accountability, and their conspicuous absence is extremely suspicious since the files exist for previous years using the same software. Removal of these files violates state law and prevents a meaningful audit, even if the Secretary wanted to conduct an audit. We must conclude that the 2020 election cycle records have been manually removed.

16. Likewise, all server security logs prior to 11:03 pm on November 4, 2020 are missing. This means that all security logs for the day after the election, on election day, and prior to election day are gone. Security logs are very important to an audit trail, forensics, and for detecting advanced persistent threats and outside attacks, especially on systems with outdated system files. These logs would contain domain controls, authentication failures, error codes, times users logged on and off, network connections to file servers between file accesses, internet connections, times, and data transfers. Other server logs before November 4, 2020 are present; therefore, there is no reasonable explanation for the security logs to be missing.

17. On November 21, 2020, an unauthorized user unsuccessfully attempted to zero out election results. This demonstrates additional tampering with data.

18. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with new ballot programming on 10/23/2020 and then again after the election on 11/05/2020. These system changes affect how ballots are read and tabulated, and our examination demonstrated a significant change in voter results using the two different programs. In accordance with the Help America Vote Act, this violates the 90-day Safe Harbor Period which prohibits changes to election systems, registries, hardware/software updates without undergoing re-certification. According to the National Conference of State Legislatures – Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.

19. The only reason to change software after the election would be to obfuscate evidence of fraud and/or to correct program errors that would de-certify the election. Our findings show that the Central Lake Township tabulator tape totals were significantly altered by utilizing two different program versions (10/23/2020 and 11/05/2020), both of which were software changes during an election which violates election law, and not just human error associated with the **Dominion Election Management System.** This is clear evidence of software generated movement of votes. The claims made on the **Office of the Secretary of State** website are false.

20. The Dominion ImageCast Precinct (ICP) machines have the ability to be connected to the internet (see Image 11). By connecting a network scanner to the ethernet port on the ICP machine and creating Packet Capture logs from the machines we examined show the ability to connect to the network, Application Programming Interface (API) (a data exchange between two different systems) calls and web (http) connections to the Election Management System server. Best practice is to disable the network interface card to avoid connection to the internet. This demonstrated a significant and fatal error in security and election integrity. Because certain files have been deleted, we have not yet found origin or destination; but our research continues.

21. Because the intentional high error rate generates large numbers of ballots to be adjudicated by election personnel, we must deduce that bulk adjudication occurred. However, because files and adjudication logs are missing, we have not yet determined where the bulk adjudication occurred or who was responsible for it. Our research continues.

22. Research is ongoing. However, based on the preliminary results, we conclude that the errors are so significant that they call into question the integrity and legitimacy of the results in the Antrim County 2020 election to the point that the results are not certifiable. Because the same machines and software are used in 48 other counties in Michigan, this casts doubt on the integrity of the entire election in the state of Michigan.

23. DNI Responsibilities: President Obama signed Executive Order on National Critical Infrastructure on 6 January 2017, stating in Section 1. Cybersecurity of Federal Networks, "The Executive Branch operates its information technology (IT) on behalf of the American people. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise." President Obama's EO further stated, effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology." Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall: (i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

This is a national security imperative. **In July 2018, President Trump strengthened President Obama's Executive Order to include requirements to ensure US election systems, processes, and its people were not manipulated by foreign meddling, either through electronic or systemic manipulation, social media, or physical changes made in hardware, software, or supporting systems.** The 2018 Executive Order. Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. 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.

We recommend that an independent group should be empaneled to determine the extent of the adjudication errors throughout the State of Michigan. This is a national security issue.

24. Michigan resident Gustavo Delfino, a former professor of mathematics in Venezuela and alumni of University of Michigan, offered a compelling affidavit [Exhibit 2] recognizing the inherent vulnerabilities in the SmartMatic electronic voting machines (software which was since incorporated into Dominion Voting Systems) during the 2004 national referendum in Venezuela (see attached declaration). After 4 years of research and 3 years of undergoing intensive peer review, Professor Delfino's paper was published in the highly respected "Statistical Science" journal, November 2011 issue (Volume 26, Number 4) with title "Analysis of the 2004 Venezuela Referendum: The Official Results Versus the Petition Signatures." The intensive study used multiple mathematical approaches to ascertain the voting results found in the 2004 Venezuelan referendum. Delfino and his research partners discovered not only the algorithm used to manipulate the results, but also the precise location in the election processing sequence where vulnerability in machine processing would provide such an opportunity. According to Prof Delfino, the magnitude of the difference between the official and the true result in Venezuela estimated at 1,370,000 votes. Our investigation into the error rates and results of the Antrim County voting tally reflect the same tactics, which have also been reported in other Michigan counties as well. This demonstrates a national security issue.

C. PROCESS

We visited Antrim County twice: November 27, 2020 and December 6, 2020.

On November 27, 2020, we visited Central Lake Township, Star Township, and Mancelona Township. We examined the Dominion Voting Systems tabulators and tabulator roles.

On December 6, 2020, we visited the Antrim County Clerk's office. We inspected and performed forensic duplication of the following:

1. **Antrim County Election Management Server** running **Dominion Democracy Suite** 5.5.3-002;

2. **Compact Flash** cards used by the local precincts in their **Dominion ImageCast Precinct;**

3. **USB memory sticks** used by the **Dominion VAT** (Voter Assist Terminals); and

4. **USB memory sticks** used for the Poll Book.

Dominion voting system is a Canadian owned company with global subsidiaries. It is owned by Staple Street Capital which is in turn owned by UBS Securities LLC, of which 3 out of their 7 board members are Chinese nationals. The Dominion software is licensed from Smartmatic which is a Venezuelan owned and controlled company. Dominion Server locations have been determined to be in Serbia, Canada, the US, Spain and Germany.

D. CENTRAL LAKE TOWNSHIP

1. On November 27, 2020, part of our forensics team visited the Central Lake Township in Michigan to inspect the **Dominion ImageCast Precint** for possible hardware issues on behalf of a local lawsuit filed by Michigan attorney Matthew DePerno on behalf of William Bailey. In our conversations with the clerk of **Central Lake Township** Ms. Judith L. Kosloski, she presented to us "two separate paper totals tape" from Tabulator ID 2.

   - One dated "Poll Opened Nov. 03/2020 06:38:48" (Roll 1);
   - Another dated "Poll Opened Nov. 06/2020 09:21:58" (Roll 2).

2. We were then told by Ms. Kosloski that on November 5, 2020, Ms. Kosloski was notified by Connie Wing of the County Clerk's Office and asked to bring the tabulator and ballots to the County Clerk's office for re-tabulation. They ran the ballots and printed "Roll 2". She noticed a difference in the votes and brought it up to the clerk, but canvasing still occurred, and her objections were not addressed.

3. Our team analyzed both rolls and compared the results. Roll 1 had **1,494** total votes and Roll 2 had **1,491** votes (Roll 2 had 3 less ballots because 3 ballots were damaged in the process.)

4. "Statement of Votes Cast from Antrim" shows that only **1,491** votes were counted, and the **3** ballots that were damaged were not entered into final results.

5. Ms. Kosloski stated that she and her assistant manually refilled out the three ballots, curing them, and ran them through the ballot counting system - but the final numbers do not reflect the inclusion of those **3** damaged ballots.

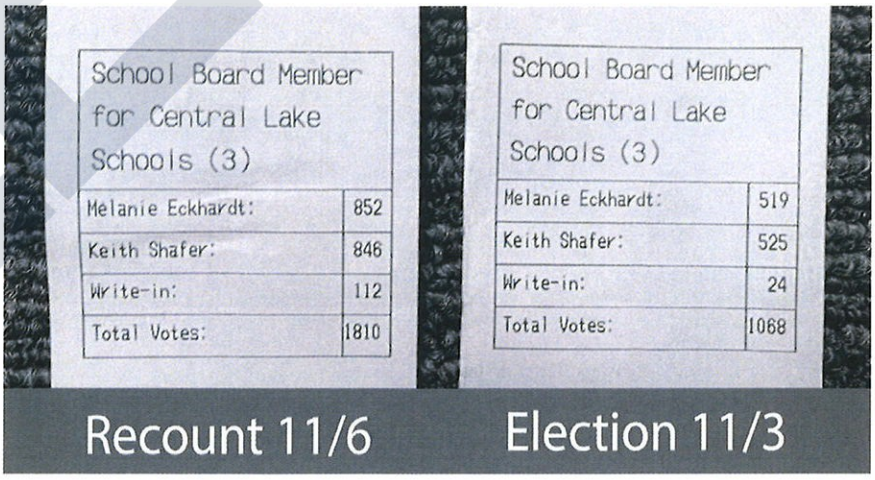
6. This is the most preliminary report of serious election fraud indicators. In comparing the numbers on both rolls, *we estimate **1,474** votes changed* across the two rolls, between the first and the second time the exact same ballots were run through the County Clerk's vote counting machine - *which is almost the same number of voters that voted in total.*

   - ***742** votes were added to* **School Board Member for Central Lake Schools (3)**
   - ***657** votes were removed from* **School Board Member for Ellsworth Schools (2)**
   - **7** votes were added to the total for **State Proposal 20-1 (1)** and out of those there were **611** votes moved between the Yes and No Categories.

7. There were incremental changes throughout the rolls with some significant adjustments between the 2 rolls that were reviewed. This demonstrates conclusively that votes can be and were changed during the second machine count after the software update. That should be impossible especially at such a high percentage to total votes cast.

8. For the **School Board Member for Central Lake Schools (3)** [Image 1] there were **742 votes** added to this vote total. Since multiple people were elected, this did not change the result of both candidates being elected, but one does see a change in who had most votes. If it were a single-person election this would have changed the outcome and demonstrates conclusively that votes can be and were changed during the second machine counting. That should be impossible.

[Image 1]:

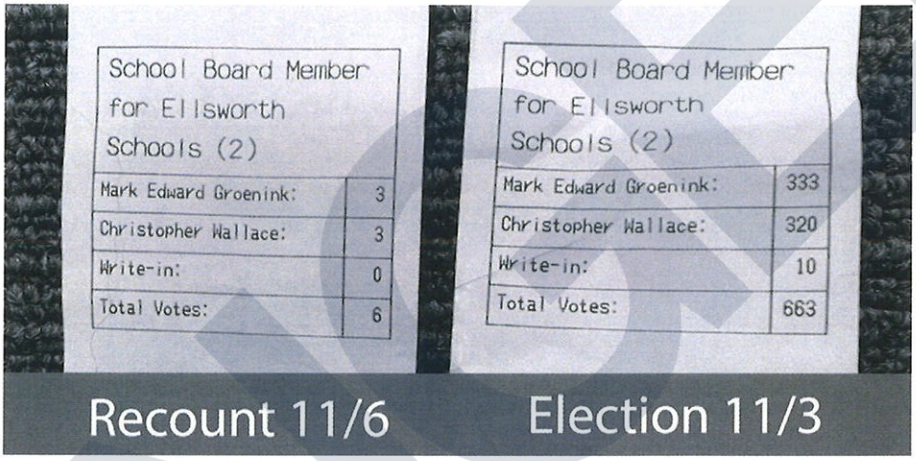


9. For the **School Board Member for Ellsworth Schools (2)** [Image 2]

- Shows ***657*** *votes being removed* from this election.
- In this case, only **3** people who were eligible to vote actually voted. Since there were **2** votes allowed for each voter to cast.
- The recount correctly shows **6** votes.

But on election night, there was a major calculation issue:

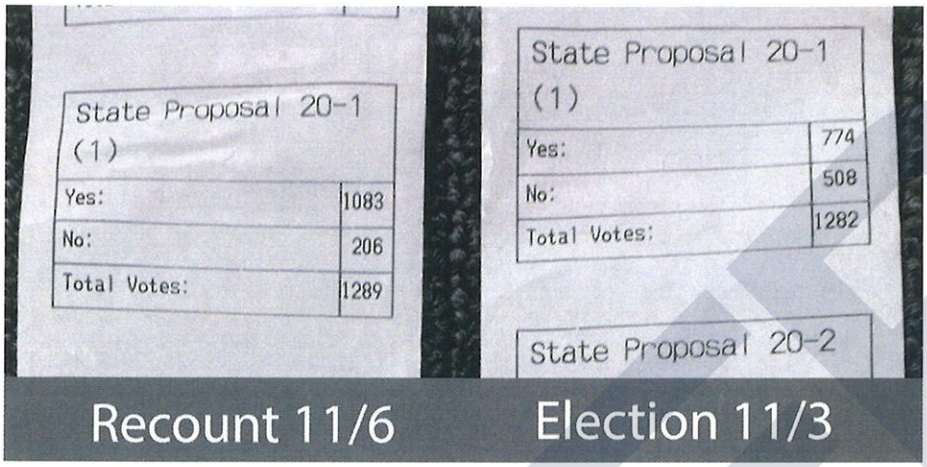
[Image 2]:



10. In **State Proposal 20-1 (1)**, [Image 3] there is a major change in votes in this category.

- There were **774 votes for YES** during the election, to **1,083 votes for YES** on the recount a change of **309 votes**.
- **7** votes were added to the total for **State Proposal 20-1 (1)** out of those there were **611** votes moved between the Yes and No Categories.

[Image 3]:



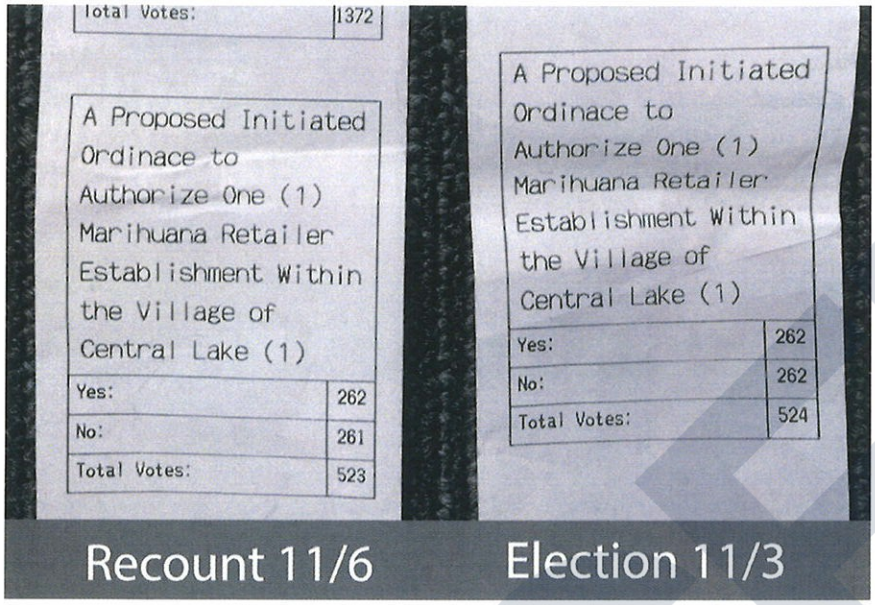
11. **State Proposal 20-1 (1)** is a fairly technical and complicated proposed amendment to the Michigan Constitution to change the disposition and allowable uses of future revenue generated from oil and gas bonuses, rentals and royalties from state-owned land. Information about the proposal: https://crcmich.org/publications/statewide-ballot- proposal-20-1-michigan-natural-resources-trust-fund

12. A Proposed Initiated **Ordinance to Authorize One (1) Marihuana (sic) Retailer Establishment Within the Village of Central Lake (1)**. [Image 4]

- On election night, it was a tie vote.
- Then, on the rerun of ballots 3 ballots were destroyed, but only one vote changed on the totals to allow the proposal to pass.

When **3 ballots were not counted** and **programming change on the tabulator was installed** the proposal **passed with 1 vote being removed from the No** vote.

[Image 4]:



13. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk. There were two USB memory sticks used, one contained the software package used to tabulate election results on November 3, 2020, and the other was programmed on November 6, 2020 with a different software package which yielded significantly different voting outcomes. The election data package is used by the **Dominion Democracy Suite** software & election management system software to upload programming information onto the Compact Flash Cards for the **Dominion ImageCast Precinct** to enable it to calculate ballot totals.

14. This software programming should be standard across all voting machines systems for the duration of the entire election if accurate tabulation is the expected outcome as required by US Election Law. This intentional difference in software programming is a design feature to alter election outcomes.

15. The election day outcomes were calculated using the original software programming on November 3, 2020. On November 5, 2020 the township clerk was asked to re-run the Central Lake Township ballots and was given no explanation for this unusual request. On November 6, 2020 the Antrim County Clerk, Sheryl Guy issued the second version of software to re-run the same Central Lake Township ballots and oversaw the process. This resulted in greater than a 60% change in voting results, inexplicably impacting every single election contest in a township with less than 1500 voters. These errors far exceed the ballot error rate standard of 1 in 250,000 ballots (.0008%) as required by federal election law.

- The original election programming files are last dated 09/25/2020 1:24pm
- The updated election data package files are last dated 10/22/2020 10:27 am.

16. As the tabulator tape totals prove, there were large numbers of votes switched from the November 3, 2020 tape to the November 6, 2020 tape. This was solely based on using different software versions of the operating program to calculate votes, not tabulate votes. This is evidenced by using same the Dominion System with two different software program versions contained on the two different USB Memory Devices.

17. The Help America Vote Act, Safe Harbor provides a 90-day period prior to elections where no changes can be made to election systems. To make changes would require recertification of the entire system for use in the election. The Dominion User Guide prescribes the proper procedure to test machines with test ballots to compare the results to validate machine functionality to determine if the **Dominion ImageCast Precinct** was programmed correctly. If this occurred a ballot misconfiguration would have been identified. Once the software was updated to the 10/22/2020 software the test ballots should have been re-run to validate the vote totals to confirm the machine was configured correctly.

18. The November 6, 2020 note from **The Office of the Secretary of State Jocelyn Benson** states: "The correct results always were and continue to be reflected on the tabulator totals tape and on the ballots themselves. Even if the error in the reported unofficial results had not been quickly noticed, it would have been identified during the county canvass. Boards of County Canvassers, which are composed of 2 Democrats and 2 Republicans, review the printed totals tape from each tabulator during the canvass to verify the reported vote totals are correct."

    - Source: https://www.michigan.gov/sos/0,4670,7-127-1640_9150-544676--,00.html

19. The **Secretary of State Jocelyn Benson's** statement is false. Our findings show that the tabulator tape totals were significantly altered by utilization of two different program versions, and not just the **Dominion Election Management System.** This is the opposite of the claim that the **Office of the Secretary of State** made on its website. The fact that these significant errors were not caught in ballot testing and not caught by the local county clerk shows that there are major inherent built-in vulnerabilities and process flaws in the **Dominion Election Management System**, and that other townships/precincts and the entire election have been affected.

20. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk office to perform forensic duplication of the **Antrim County Election Management Server** running **Dominion Democracy Suite** 5.5.3-002.

21. Forensic copies of the **Compact Flash** cards used by the local precincts in their **Dominion ImageCast Precinct** were inspected, **USB memory sticks** used by the **Dominion VAT** (Voter Assist Terminals) and the **USB memory sticks** used for the Poll Book were forensically duplicated.

22. We have been told that the ballot design and configuration for the **Dominion ImageCast Precinct** and VAT were provided by **ElectionSource.com** which is which is owned by MC&E, Inc of Grand Rapids, MI.

E. MANCELONA TOWNSHIP

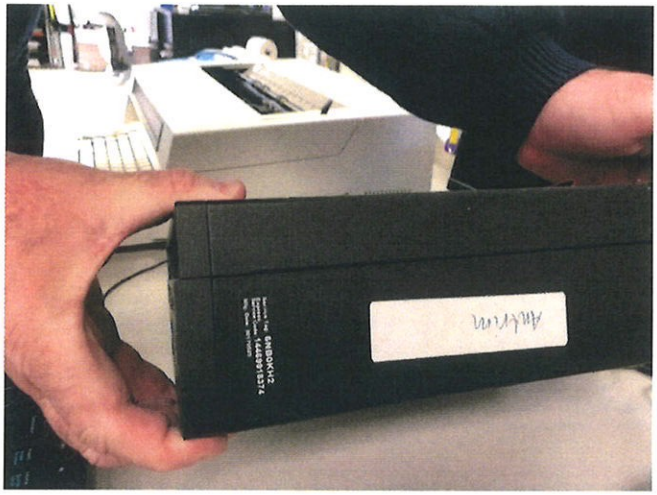
1. In Mancelona township, problems with software versions were also known to have been present. Mancelona elections officials understood that ballot processing issued were not accurate and used the second version of software to process votes on 4 November, again an election de-certifying event, as no changes to the election system are authorized by law in the 90 days preceding elections without re-certification.

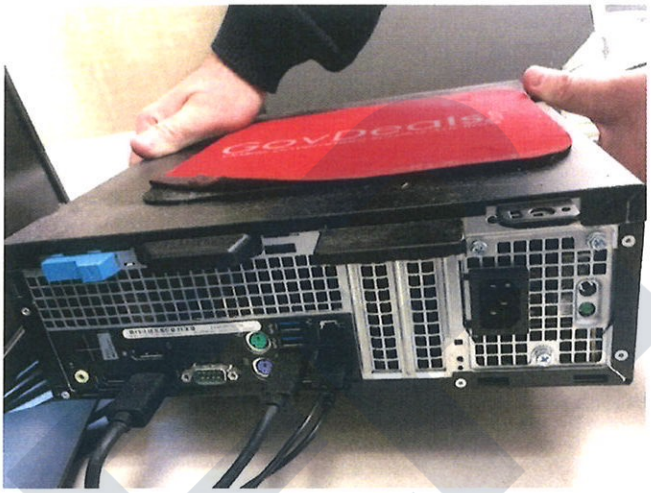
2. Once the 10/22/2020 software update was performed on the Dominion ImageCast Precinct the test ballot process should have been performed to validate the programming. There is no indication that this procedure was performed.

F. ANTRIM COUNTY CLERK'S OFFICE

1. Pursuant to a court ordered inspection, we participated in an onsite collection effort at the Antrim County Clerk's office on December 6, 2020. [Image 5]:

Among other items forensically collected, the Antrim County Election Management Server (EMS) with Democracy Suite was forensically collected. [Images 6 and 7].





The EMS (Election Management Server) was a:

Dell Precision Tower 3420.

Service Tag: 6NB0KH2

The EMS contained 2 hard drives in a RAID-1 configuration. That is the 2 drives redundantly stored the same information and the server could continue to operate if either of the 2 hard drives failed. The EMS was booted via the Linux Boot USB memory sticks and both hard drives were forensically imaged.

At the onset of the collection process we observed that the initial program thumb drive was not secured in the vault with the CF cards and other thumbdrives. We watched as the County employees, including Clerk Sheryl Guy searched throughout the office for the missing thumb drive. Eventually they found the missing thumb drive in an unsecured and unlocked desk drawer along with multiple other random thumb drives. This demonstrated a significant and fatal error in security and election integrity.

G. FORENSIC COLLECTION

We used a built for purpose Linux Boot USB memory stick to boot the EMS in a forensically sound mode. We then used Ewfacquire to make a forensic image of the 2 independent internal hard drives.

Ewfacquire created an E01 file format forensic image with built-in integrity verification via MD5 hash.

We used Ewfverify to verify the forensic image acquired was a true and accurate copy of the original disk. That was done for both forensic images.

H. ANALYSIS TOOLS

X-Ways Forensics: We used X-Ways Forensics, a commercial Computer Forensic tool, to verify the image was useable and full disk encryption was not in use. In particular we confirmed that Bit locker was not in use on the EMS.

Other tools used: PassMark – OSForensics, Truxton - Forensics, Cellebrite – Physical Analyzer, Blackbag-Blacklight Forensic Software, Microsoft SQL Server Management Studio, Virtual Box, and miscellaneous other tools and scripts.

I. SERVER OVERVIEW AND SUMMARY

1. Our initial audit on the computer running the Democracy Suite Software showed that standard computer security best practices were not applied. These minimum-security standards are outlined the 2002 HAVA, and FEC Voting System Standards – it did not even meet the minimum standards required of a government desktop computer.

2. The election data software package USB drives (November 2020 election, and November 2020 election updated) are secured with bitlocker encryption software, but they were not stored securely on-site. At the time of our forensic examination, the election data package files were already moved to an unsecure desktop computer and were residing on an unencrypted hard drive. This demonstrated a significant and fatal error in security and election integrity. Key Findings on Desktop and Server Configuration: - There were multiple Microsoft security updates as well as Microsoft SQL Server updates which should have been deployed, however there is no evidence that these security patches were ever installed. As described below, many of the software packages were out of date and vulnerable to various methods of attack.

    a) Computer initial configuration on 10/03/2018 13:08:11:911

    b) Computer final configuration of server software on 4/10/2019

    c) Hard Drive not Encrypted at Rest

    d) Microsoft SQL Server Database not protected with password.

    e) Democracy Suite Admin Passwords are reused and share passwords.

    f) Antivirus is 4.5 years outdated

    g) Windows updates are 3.86 years out of date.

    h) When computer was last configured on 04/10/2019 the windows updates were 2.11 years out of date.

    i) User of computer uses a Super User Account.

3. The hard drive was not encrypted at rest – which means that if hard drives are removed or initially booted off an external USB drive the files are susceptible to manipulation directly. An attacker is able to mount the hard drive because it is unencrypted, allowing for the manipulation and replacement of any file on the system.

4. The Microsoft SQL Server database files were not properly secured to allow modifications of the database files.

5. The Democracy Suite Software user account logins and passwords are stored in the unsecured database tables and the multiple Election System Administrator accounts share the same password, which means that there are no audit trails for vote changes, deletions, blank ballot voting, or batch vote alterations or adjudication.

6. Antivirus definition is 1666 days old on 12/11/2020. Antrim County updates its system with USB drives. USB drives are the most common vectors for injecting malware into computer systems. The failure to properly update the antivirus definition drastically increases the harm cause by malware from other machines being transmitted to the voting system.

7. Windows Server Update Services (WSUS) Offline Update is used to enable updates the computer – which is a package of files normally downloaded from the internet but compiled into a program to put on a USB drive to manually update server systems.

8. Failure to properly update the voting system demonstrates a significant and fatal error in security and election integrity.

9. There are 15 additional updates that should have been installed on the server to adhere to Microsoft Standards to fix known vulnerabilities. For the 4/10/2019 install, the most updated version of the update files would have been 03/13/2019 which is 11.6.1 which is 15 updates newer than 10.9.1

This means the updates installed were 2 years, 1 month, 13 days behind the most current update at the time. This includes security updates and fixes. This demonstrated a significant and fatal error in security and election integrity.

- Wed 04/10/2019 10:34:33.14 - Info: Starting WSUS Offline Update (v. 10.9.1)
- Wed 04/10/2019 10:34:33.14 - Info: Used path "D:\WSUSOFFLINE1091_2012R2_W10\cmd\" on EMSSERVER (user: EMSADMIN)
- Wed 04/10/2019 10:34:35.55 - Info: Medium build date: 03/10/2019

- Found on c:\Windows\wsusofflineupdate.txt
- *WSUS Offline Update (v.10.9.1) was created on 01/29/2017

*WSUS information found here https://download.wsusoffline.net/

10. Super User Administrator account is the primary account used to operate the **Dominion Election Management System** which is a major security risk. The user logged in has the ability to make major changes to the system and install software which means that there is no oversight to ensure appropriate management controls – i.e. anyone who has access to the shared administrator user names and passwords can make significant changes to the entire voting system. The shared usernames and passwords mean that these changes can be made in an anonymous fashion with no tracking or attribution.

J. ERROR RATES

1. We reviewed the Tabulation logs in their entirety for 11/6/2020. The election logs for Antrim County consist of 15,676 total lines or events.
   - Of the 15,676 there were a total of 10,667 critical errors/warnings or a 68.05% error rate.
   - Most of the errors were related to configuration errors that could result in overall tabulation errors or adjudication. These 11/6/2020 tabulation totals were used as the official results.

2. For examples, there were 1,222 ballots **reversed** out of 1,491 total ballots cast, thus resulting in an 81.96% rejection rate. Some of which were reversed due to "Ballot's size exceeds maximum expected ballot size".
   - According to the NCSL, Michigan requires testing by a federally accredited laboratory for voting systems. In section 4.1.1 of the Voluntary Voting Systems Guidelines (VVSG) Accuracy Requirements a. **All systems shall achieve a report total error rate of no more than one in 125,000**.
   - https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf
   - In section 4.1.3.2 Memory Stability of the VVSG it states that **Memory devices used to retain election management data shall have demonstrated error free data retention for a period of 22 months**.
   - In section 4.1.6.1 Paper-based System Processing Requirements sub-section a. of the VVSG it states "The ability of the system to produce and receive electronic signals from the scanning of the ballot, perform logical and numerical operations upon these data, and reproduce the contents of memory when required **shall** be sufficiently free of **error** to enable

satisfaction of the system-level accuracy requirement indicated in Subsection 4.1.1."

- These are not human errors; this is definitively related to the software and software configurations resulting in error rates far beyond the thresholds listed in the guidelines.

3. A high "error rate" in the election software (in this case 68.05%) reflects an algorithm used that will weight one candidate greater than another (for instance, weight a specific candidate at a 2/3 to approximately 1/3 ratio). In the logs we identified that the RCV or Ranked Choice Voting Algorithm was enabled (see image below from the Dominion manual). This allows the user to apply a weighted numerical value to candidates and change the overall result. The declaration of winners can be done on a basis of points, not votes. [Image 8]:

> choice voting results are evaluated on a district per district basis and each district has a set number of points (100). Elimination and declaration of winners is done on basis of points, not votes.

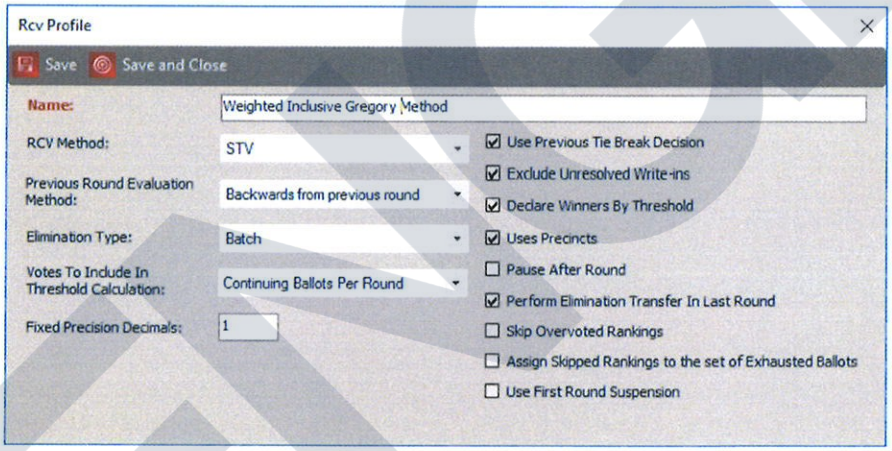
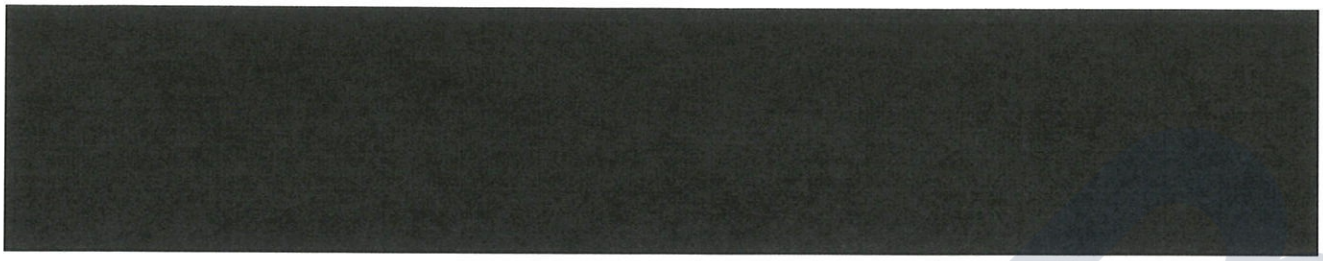


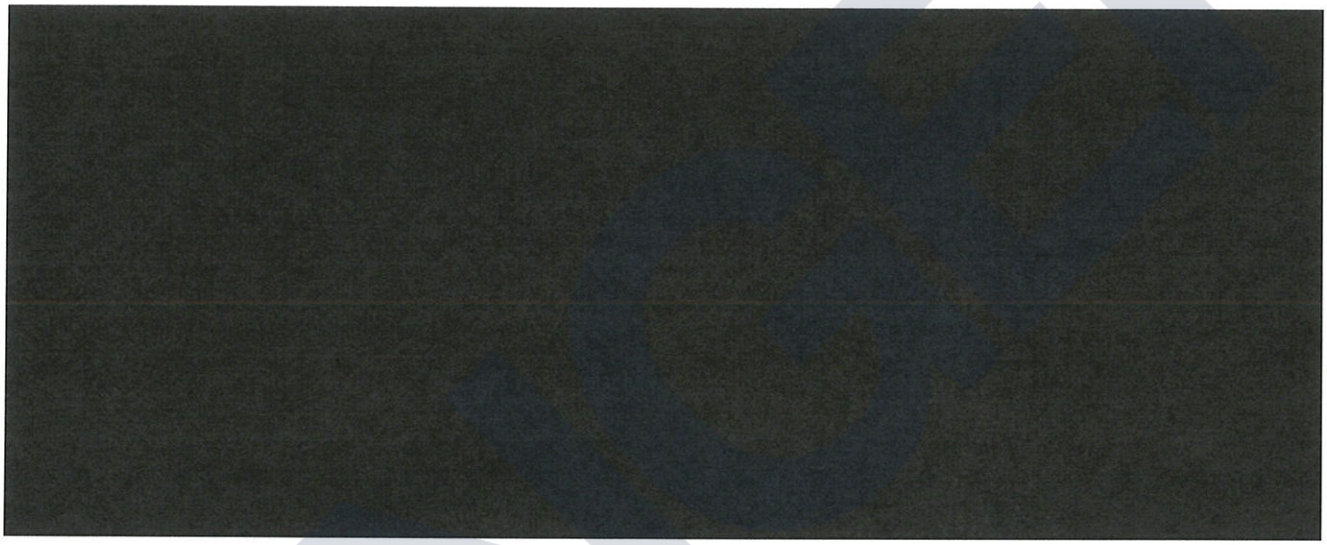
Figure 11-3: RCV Profile screen

4. The Dominion software configuration logs in the Divert Options, shows that all write-in ballots were flagged to be diverted automatically for adjudication. This means that all write-in ballots were sent for "adjudication" by a poll worker or election official to process the ballot based on voter "intent". Adjudication files allow a computer operator to decide to whom to award those votes (or to trash them).

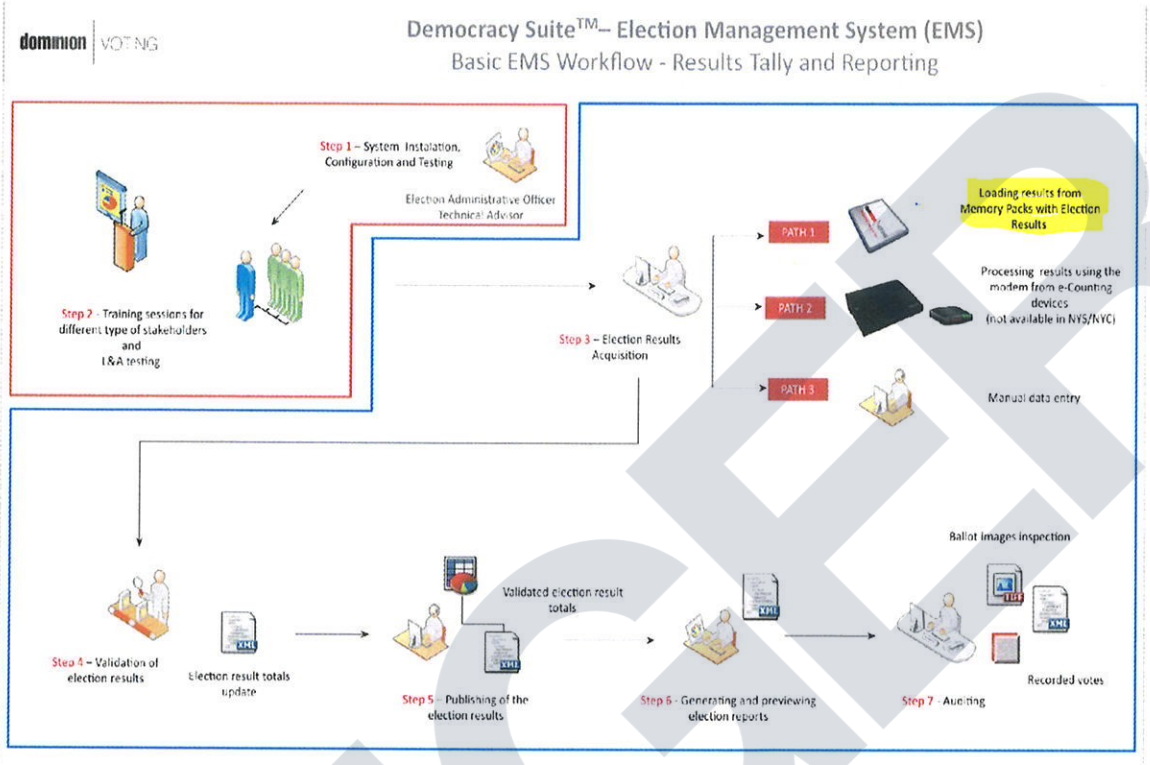
5. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. [Image 9]:



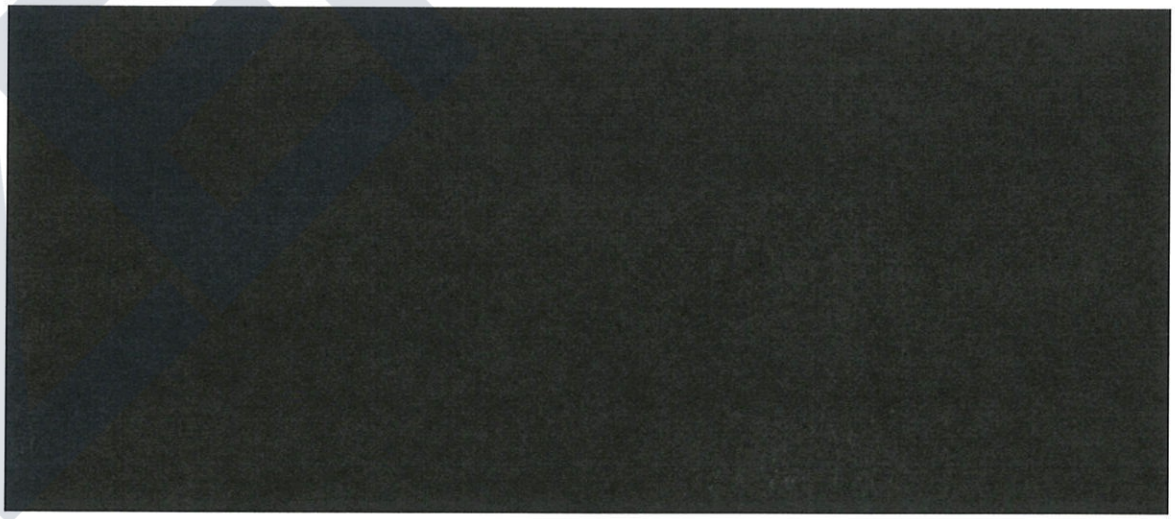
6. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. This gives the system operators carte blanche to adjudicate ballots, in this case 81.96% of the total cast ballots with no audit trail or oversight. [Image 10]:



7. On 12/8/2020 Microsoft issued 58 security patches across 10+ products, some of which were used for the election software machine, server and programs. Of the 58 security fixes 22, were patches to remote code execution (RCE) vulnerabilities. [Image 11]:



8. We reviewed the Election Management System logs (EmsLogger) in their entirety from 9/19/2020 through 11/21/2020 for the Project: Antrim November 2020. There were configuration errors throughout the set-up, election and tabulation of results. The last error for Central Lake Township, Precinct 1 occurred on 11/21/2020 at 14:35:11 System.Xml.XmlException System.Xml.XmlException: The ' ' character, hexadecimal value 0x20, cannot be included in a name. Bottom line is that this is a calibration that rejects the vote (see picture below). [Image 12]:



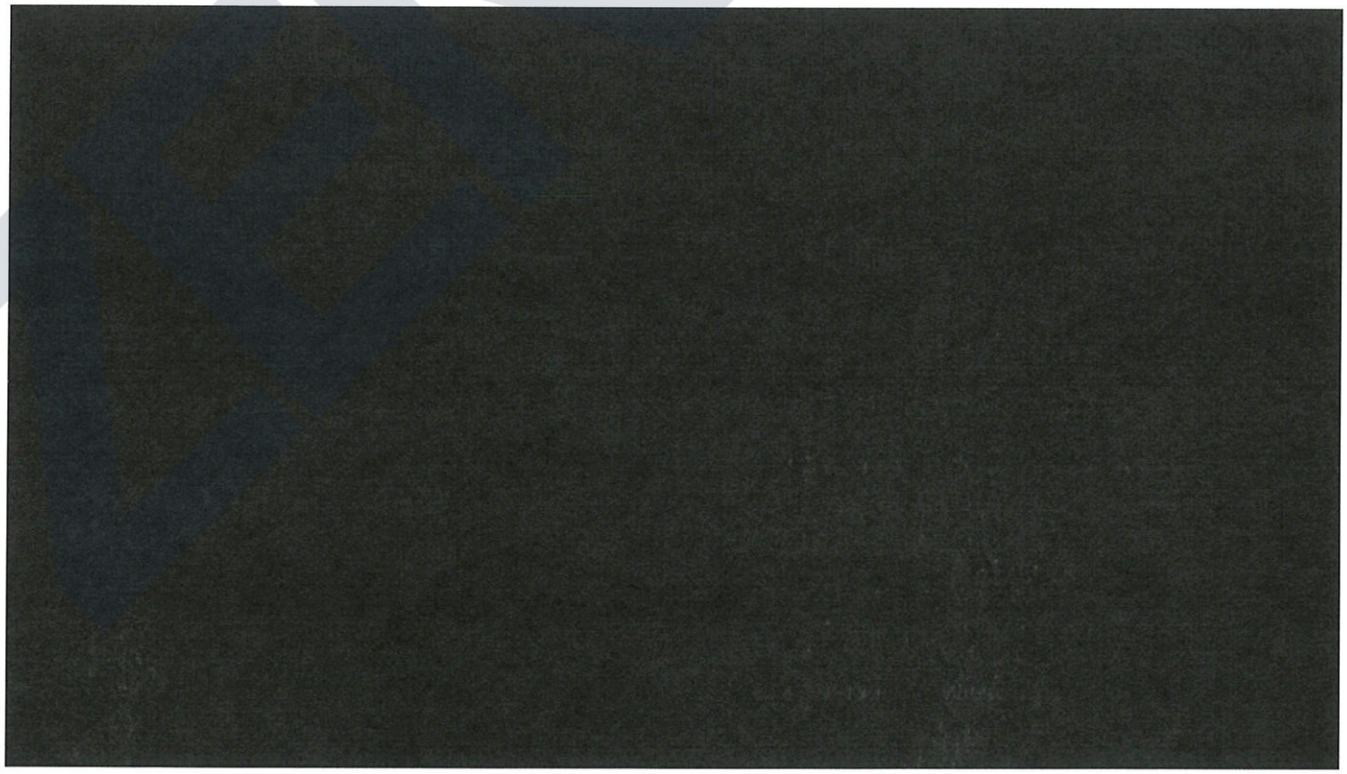
Notably 42 minutes earlier on Nov 21 2020 at 13:53:09 a user attempted to zero out election results. Id:3168 EmsLogger - There is no permission to {0} - Project: User: Thread: 189. This is direct proof of an attempt to tamper with evidence.

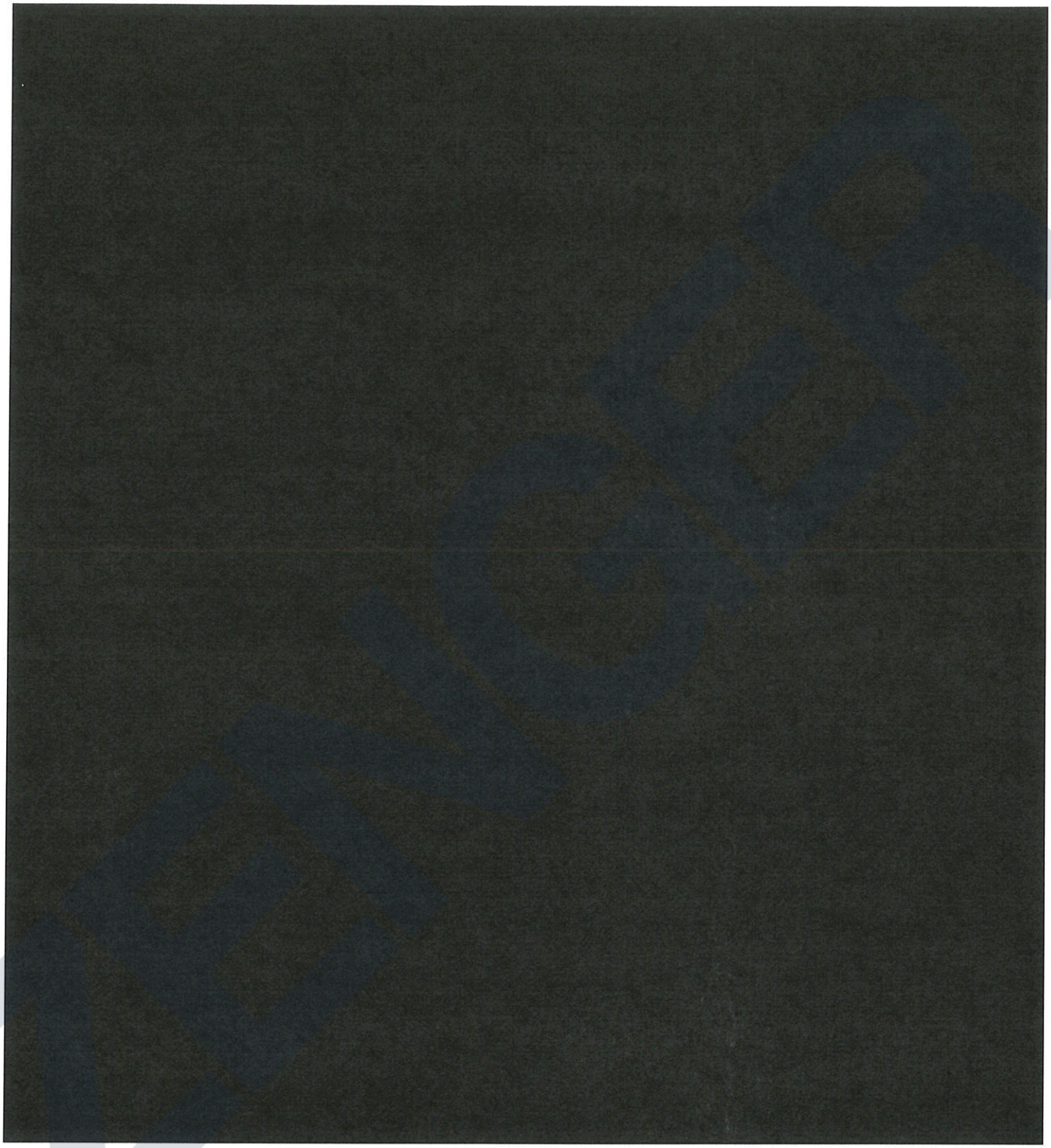
9. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with updated new programming on 10/23/2020 and again after the election on 11/05/2020. As previously mentioned, this violates the HAVA safe harbor period.

   Source: C:\Program Files\Dominion Voting Systems\Election Event Designer\Log\Info.txt

   - Dominion Imagecast Precinct Cards Programmed with 9/25/2020 programming on 09/29/2020, 09/30/2020, and 10/12/2020.
   - Dominion Imagecast Precinct Cards Programmed with New Ballot Programming dated 10/22/2020 on 10/23/2020 and after the election on 11/05/2020

   Excerpt from 2020-11-05 showing "ProgramMemoryCard" commands.





10. Analysis is ongoing and updated findings will be submitted as soon as possible. A summary of the information collected is provided below.

10|12/07/20 18:52:30| Indexing completed at Mon Dec 7 18:52:30 2020
12|12/07/20 18:52:30| INDEX SUMMARY
12|12/07/20 18:52:30| Files indexed: 159312

12|12/07/20 18:52:30| Files skipped: 64799
12|12/07/20 18:52:30| Files filtered: 0
12|12/07/20 18:52:30| Emails indexed: 0
12|12/07/20 18:52:30| Unique words found: 5325413
12|12/07/20 18:52:30| Variant words found: 3597634
12|12/07/20 18:52:30| Total words found: 239446085
12|12/07/20 18:52:30| Avg. unique words per page: 33.43
12|12/07/20 18:52:30| Avg. words per page: 1503
12|12/07/20 18:52:30| Peak physical memory used: 2949 MB
12|12/07/20 18:52:30| Peak virtual memory used: 8784 MB
12|12/07/20 18:52:30| Errors: 10149
12|12/07/20 18:52:30| Total bytes scanned/downloaded: 1919289906

Dated: December 13, 2020

Russell Ramsland

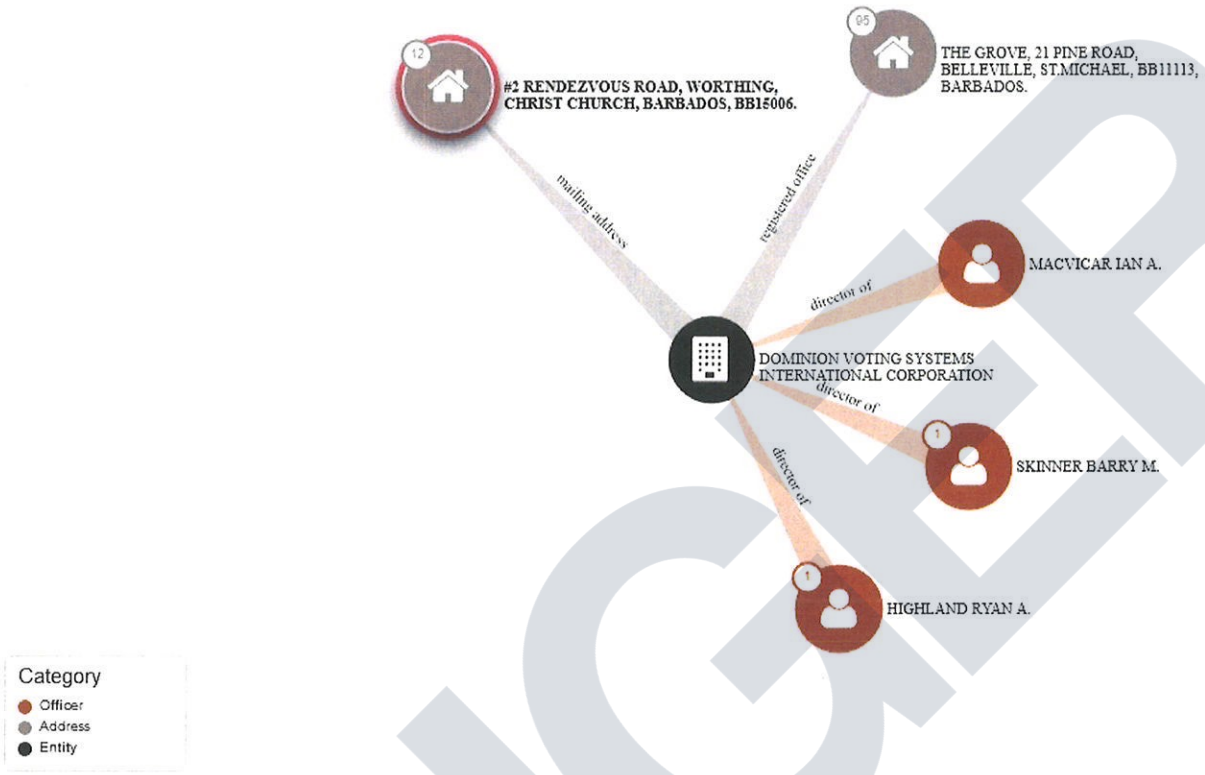
Declaration of [redacted]

1. My name is [redacted], and I am a resident of [redacted]. I hold an [redacted] from [redacted] University, and a [redacted] from [redacted] University. I am [redacted]. Our emphasis is on digital forensics and incident response (DFIR) cybersecurity, analysis of publicly available information (PAI), penetration testing of networks, and problem solving through operations integration. We use state-of-the-art tools and employ a wide variety of cyber and cyber-forensic analysts. My colleagues and I are currently contracted to a cyber-security and forensics firm that focuses on election systems.

2. We have examined the various companies, networks, structures, machines, and related global infrastructures directly tied to the 2020 US General Election.

3. This is a preliminary report on the various aspects of FOREIGN INTERFERENCE as defined by Executive Order 13848 issued on September 12, 2018.
    a. Section 8 (f) defines the term "foreign interference," with respect to an election, to include "any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions."

ICIJ **OFFSHORE LEAKS DATABASE**



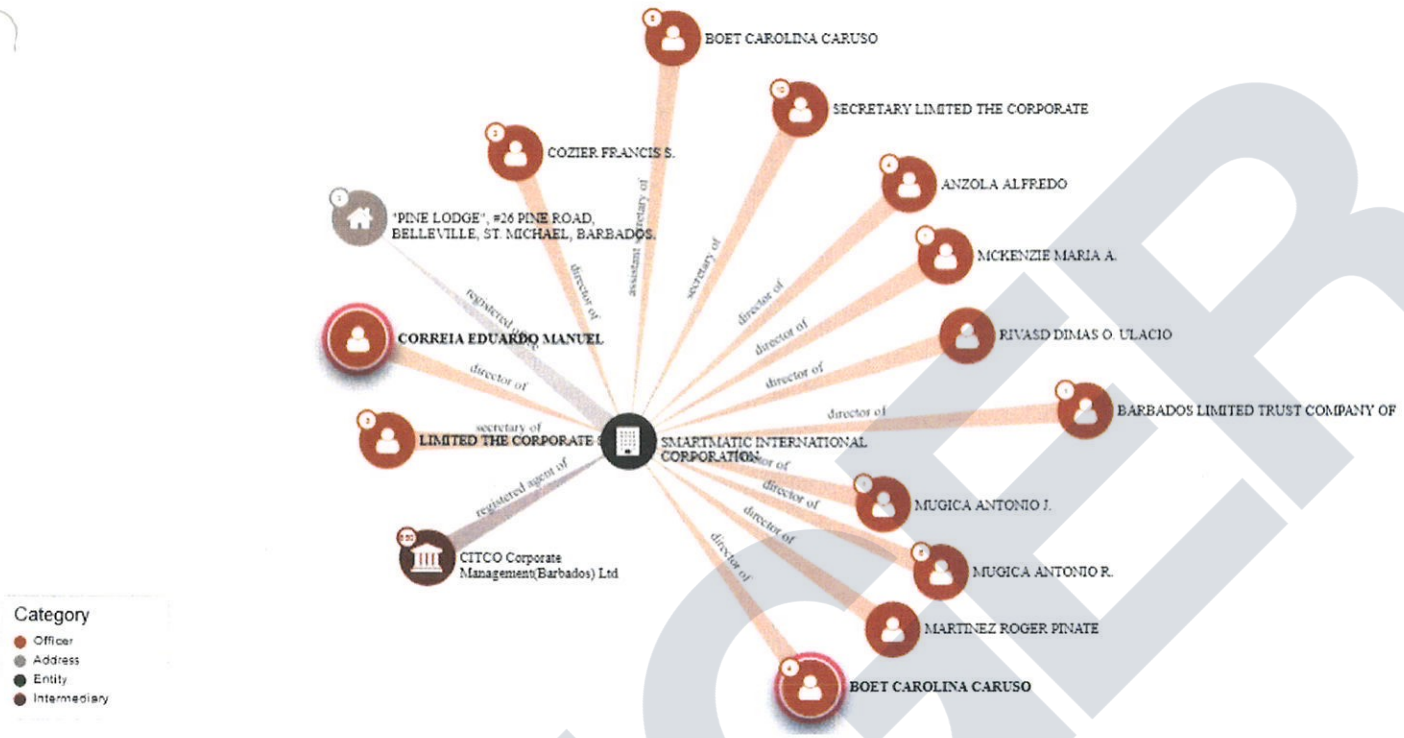
https://offshoreleaks.icij.org/nodes/101724285

SMARTMATIC INTERNATIONAL CORPORATION

Connected to **1 address**
Connected to **13 officers**
Connected to **1 intermediary**

Incorporated: 29-SEP-2004
Registered in: Barbados
Linked countries: Barbados

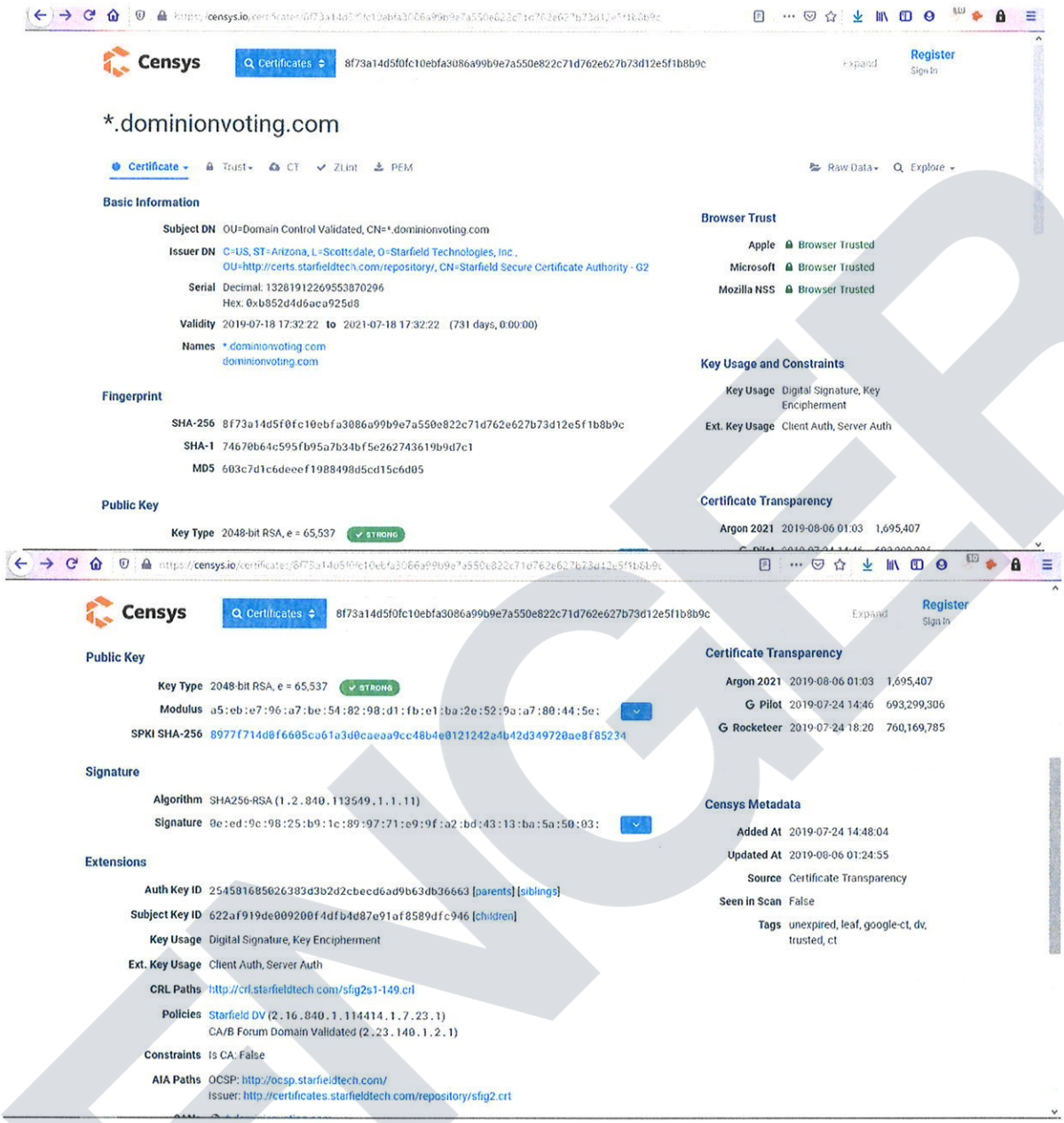
Data from: Paradise Papers - Barbados corporate registry
Barbados corporate registry data is current through 2016
Search in opencorporates
Got a tip? Help ICIJ investigate: contact us or leak to us securely



ominion Certificates

25. Dominion can be seen using open-source methodology that the SSL certificates from *.dominionvoting.com were registered on the 24th of July 2019. This SSL certificate were used multiple times from locations ranging from Canada, Serbia, and the United States. These images verify that Dominion systems were connected to foreign systems across the globe. Also seen is that the SSL certificate is used for the email server that was the same for the secure HTTP connections.

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c



Censys | Certificates | 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c | Expand | Register | Sign In

*.dominionvoting.com

Certificate | Trust | CT | ZLint | PEM | Raw Data | Explore

Basic Information

Subject DN OU=Domain Control Validated, CN=*.dominionvoting.com

Issuer DN C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc., OU=http://certs.starfieldtech.com/repository/, CN=Starfield Secure Certificate Authority - G2

Serial Decimal: 1328191226955870296
Hex: 0xb852d4d6aca925d8

Validity 2019-07-18 17:32:22 to 2021-07-18 17:32:22 (731 days, 0:00:00)

Names *.dominionvoting.com
dominionvoting.com

Fingerprint

SHA-256 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

SHA-1 74670b64c595fb95a7b34bf5e262743619b9d7c1

MD5 603c7d1c6deeef1988498d5cd15c6d05

Public Key

Key Type 2048-bit RSA, e = 65,537 STRONG

Browser Trust

Apple Browser Trusted

Microsoft Browser Trusted

Mozilla NSS Browser Trusted

Key Usage and Constraints

Key Usage Digital Signature, Key Encipherment

Ext. Key Usage Client Auth, Server Auth

Certificate Transparency

Argon 2021 2019-08-06 01:03 1,695,407

Censys | Certificates | 8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c | Expand | Register | Sign In

Public Key

Key Type 2048-bit RSA, e = 65,537 STRONG

Modulus a5:eb:e7:96:a7:be:54:82:98:d1:fb:e1:ba:2e:52:9a:a7:80:44:5e:

SPKI SHA-256 8977f714d8f6605ca61a3d0caeaa9cc48b4e0121242a4b42d349720ae8f85234

Signature

Algorithm SHA256-RSA (1.2.840.113549.1.1.11)

Signature 0e:ed:9c:98:25:b9:1c:89:97:71:e9:9f:a2:bd:43:13:ba:5a:50:03:

Extensions

Auth Key ID 2545816850626383d3b2d2cbecd6ad9b63db36663 [parents] [siblings]

Subject Key ID 622af919de009200f4dfb4d87e91af8589dfc946 [children]

Key Usage Digital Signature, Key Encipherment

Ext. Key Usage Client Auth, Server Auth

CRL Paths http://crl.starfieldtech.com/sfig2s1-149.crl

Policies Starfield DV (2.16.840.1.114414.1.7.23.1)
CA/B Forum Domain Validated (2.23.140.1.2.1)

Constraints Is CA: False

AIA Paths OCSP: http://ocsp.starfieldtech.com/
Issuer: http://certificates.starfieldtech.com/repository/sfig2.crt

Certificate Transparency

Argon 2021 2019-08-06 01:03 1,695,407

G Pilot 2019-07-24 14:46 693,299,306

G Rocketeer 2019-07-24 18:20 760,169,785

Censys Metadata

Added At 2019-07-24 14:48:04

Updated At 2019-08-06 01:24:55

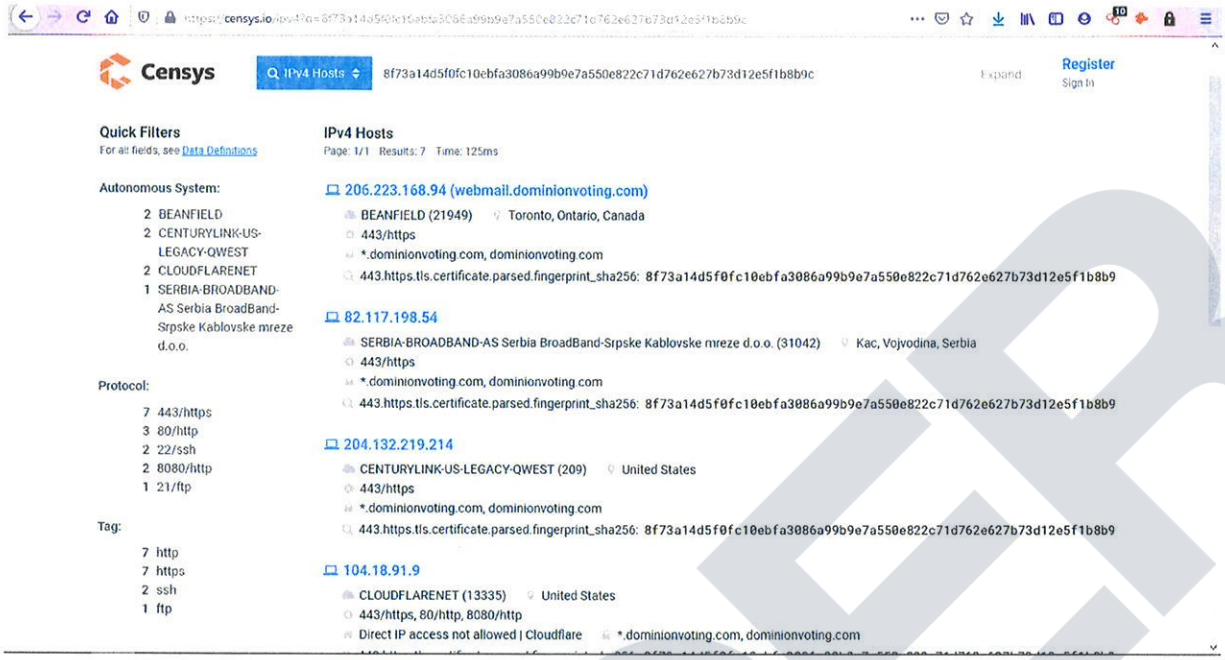
Source Certificate Transparency

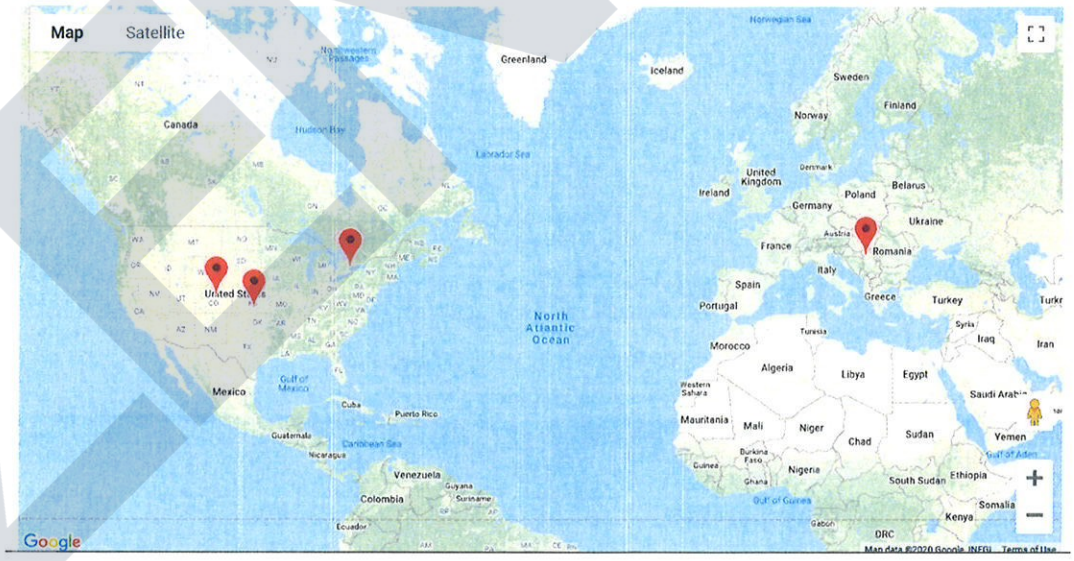
Seen in Scan False

Tags unexpired, leaf, google-ct, dv, trusted, ct

ıll share:

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9





mail ip address:

206.223.168.94

Serbian ip address

82.117.198.54
Dominion site
204.132.219.214
loudflare link
104.18.91.9
Canadian ip address
206.223.190.85
Denver ip address
204.132.121.11

Page: 1/1 Results: 7 Time: 155ms
206.223.168.94 (webmail.dominionvoting.com)
BEANFIELD (21949) Toronto, Ontario, Canada
443/https
*.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
82.117.198.54
SERBIA-BROADBAND-AS Serbia BroadBand-Srpske Kablovske mreze d.o.o. (31042) Kac, Vojvodina, Serbia
443/https
*.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
204.132.219.214
CENTURYLINK-US-LEGACY-QWEST (209) United States
443/https
*.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
104.18.91.9
CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
104.18.90.9
CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
206.223.190.85 (206-223-190-85.beanfield.net)
BEANFIELD (21949) Toronto, Ontario, Canada
2/ssh, 443/https
*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c
204.132.121.11 (204-132-121-11.dia.static.qwest.net)
CENTURYLINK-US-LEGACY-QWEST (209) Denver, Colorado, United States
21/ftp, 22/ssh, 443/https, 80/http
DVS Fileshare *.dominionvoting.com, dominionvoting.com
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

Supply Chain Concerns

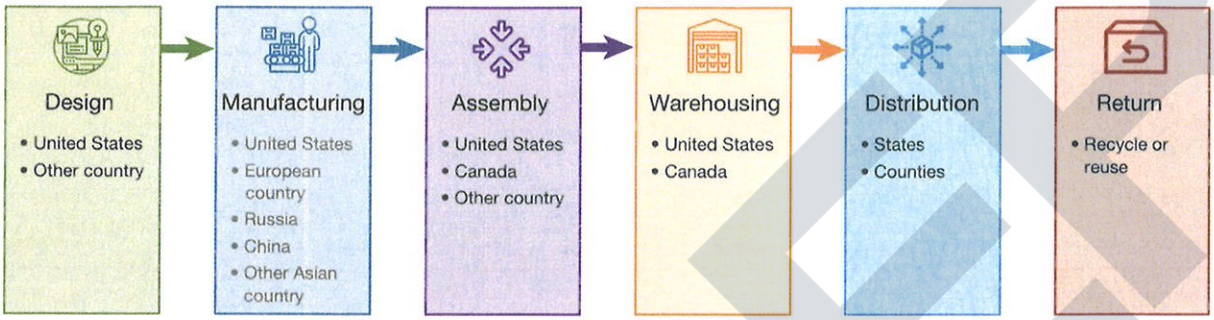
28. One in five components used in voting machines are from China-based companies

29. On January 6, 2017 DHS Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.

    a. This means that election infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state and local election officials, but only for those who request it. Further, the designation makes clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer. Finally, a designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information.

30. With that in mind, it is incredible that the Election equipment used in the November 3, 2020 election was manufactured in **Russia, China** and undisclosed Asian and European Countries (see below).

Phases and Participants in a Supply Chain for Election Equipment for Use in the United States



SOURCE: The countries listed are found in Interos, 2019.

Reference:

https://us-cert.cisa.gov/sites/default/files/2020-10/AA20-304A-Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data.pdf

https://www.whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/

https://www.jstor.org/stable/resrep26524?seq=13#metadata_info_tab_contents

https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[redacted]

Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.

2. I [redacted]

3. I am a US citizen and I reside [redacted] in the United States of America.

4. Whereas the Dominion and Edison Research systems exist in the internet of things, many of their employees and Corporate employees have had their Personally identifiable information, (PII) posted publicly prior to the election and had since deleted information from public websites as well as their company websites. However searching though historic records online, much of their information can be retrieved. The following has to do with key employees and the tied to foreign nations:

Andy Huang, Core Infrastructure Manager of IT at Dominion Voting, previously worked for CCP China Telecom in 1998-2002, has a (jewelry? shell) company called Oriental Net Consulting

Andy Huang, Core Infrastructure Manager of IT at Dominion Voting, previously worked for CCP China Telecom in 1998-2002, has a (jewelry? shell) company called OrientalNet Consulting

Andy Huang currently works as the Core Infrastructure Manager of Information Technology at Dominion Voting Systems. Earlier, he worked at China Telecom for four years between 1998 and 2002. The company is wholly run by the Chinese government. Huang indicates on his LinkedIn that he studied at Dalhousie University in Halifax, Canada.

During his tenure with China Telecom, Huang was tasked with several projects including 'Xiamen Metropolitan-are broadband network', 'Xiamen IDC Project', and 'OA Intranet infrastructure reformation project'. The exact role Huang played in these projects is not known. Huang has also worked with Cisco, a company that contributed significantly to the establishment of the Great Chinese Firewall.

The U.S. Department of Defense has identified China Telecom as having collaborated with the Chinese military for over 20 years. In addition, the U.S. Department of Homeland Security and several other federal agencies had called for a complete ban on China Telecom in April due to national security concerns. Ever since his history with China Telecom became public knowledge, Huang has deleted both China Telecom and Dominion as employers from his LinkedIn profile.

Andy Huang's Chinese pinyin name is Xiaolong Huang as per Canadian incorporation records of OrientalNet Consulting that is indicated in his LinkedIn profile. The addresses and names match when cross-referenced against multiple sources.

OrientalNet Consulting returns as a jewelry trading company on a business listing site, with Andy's name and business details. The address and phone number has changed since.

Searching "OrientalNet Consulting" also returns us "ORIENTALNET CONSULTING LTD. CHINA BRANCH" at another business listing site for Chinese businesses with the below details:
"Room 302, Building 4, No.25 Hexiangdong Rd, Xiamen, China (Mainland), Fujian
PHONE NUMBER
86-592-8133881
FAX
86-592-5971483
ESTABLISHMENT YEAR 2001

Orientalnet consulting Ltd. China trading branch is a professional manufacturer and exporter specializing in paper products. "

Joyce Zeng is listed as a contact for Orientalnet Consulting Ltd. China Branch. **There is no proof that Andy Huang's OrientalNet Consulting is linked to Orientalnet Consulting China Branch, but one thing that is extremely questionable is the jewelry trading company that is linked to him. Was this a shell company?**

https://thenationalpulse.com/news/dominion-techie-worked-for-ccp-military-proxy-flagged-by-u-s-govt-for-malicious-cyber-activity/

https://visiontimes.com/2020/11/29/dominion-employee-previously-worked-for-chinese-state-company.html

https://www.can1business.com/company/Active/Orientalnet-Consulting-Ltd

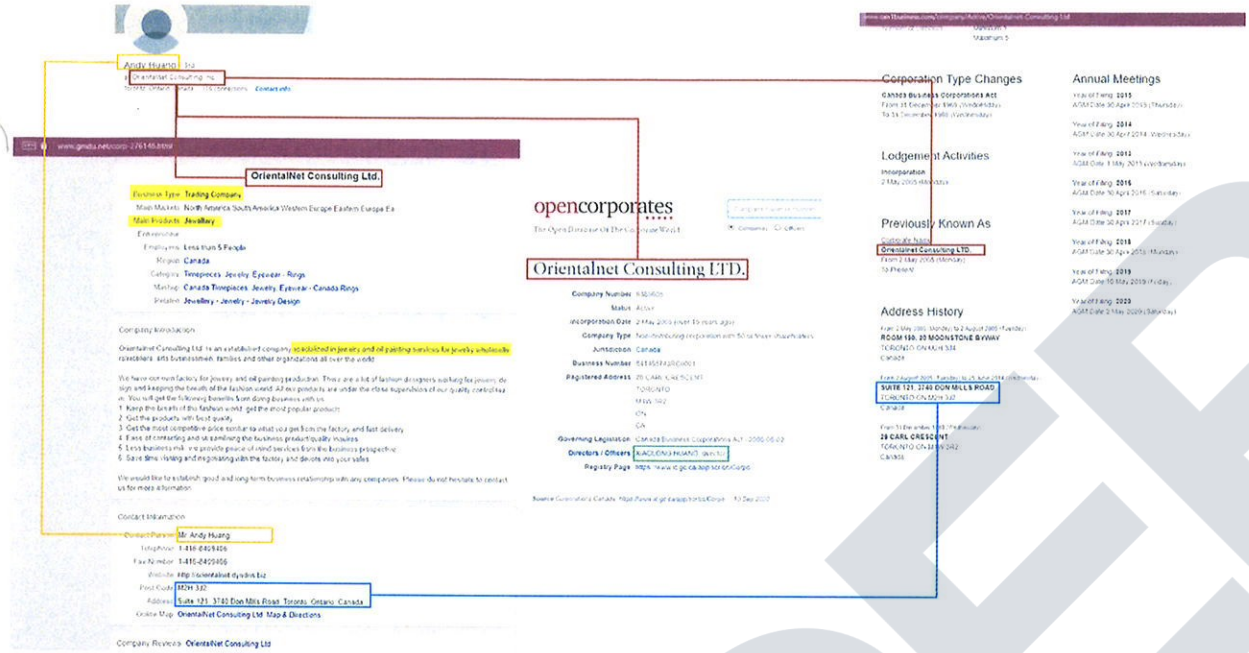
https://www.gmdu.net/corp-276148.html / https://archive.vn/fgioe

http://www.chinayello.com/company/54513/ORIENTALNET_CONSULTING_LTD_CHINA_BRANCH / https://archive.vn/GYWOY

https://www.linkedin.com/in/andy-huang-0886636/

http://www.bizearch.com/company/Orientalnet_Consulting_Ltd_China_Branch_24063.htm
Andy's LinkedIn prior to him removing a lot of his work history

https://twitter.com/BenKTallmadge/status/1330150320530452487/



VPN www.linkedin.com/in/andy-huang-0886636/

Search

Home · My Network · Jobs · Mess

Andy Huang · 3rd

at Orientalnet Consulting Inc.

Toronto, Ontario, Canada · 116 connections · **Contact info**

Dalhousie University

About

* 10 years experience in LAN & WAN with Cisco routers and switches in complex UNIX & Windows Server environment.
* 10 years Telecom experience and excellent customer service experience.
* 6 years experience in complex Converged NOC operation support environment.
* Excellent experience in Avaya & Cisco IPT, Call Manager, Unity configuration
* Excellent experience in Avaya S87xx, S8500, S8300 media server, G700, G350, G250 media gateway, 46xx, 96xx IP phone, IP agent
* Profound understand of ISDN, T1 signaling, traditional PSTN/Mobile network
* Routed and routing protocols: IP, IPX, OSPF, BGP, EIGRP, RIP.
* Excellent experience in ATM, FRAME RELAY, DDR, ISDN, PPP, OC3, E-1/T-1.
* Excellent experience in Multi layer switching, Gigabit Ethernet, VLAN, PVLAN, STP, 802.1p/q, FEC, wireless networking.
* Excellent experience in network and system security: Firewall (PIX), VPN.
* Excellent experience in Network Management Tools: SMARTS/Remedy, Cisco ACS Radius server and SNIFFER.
* Excellent network design experience: use Powerpoint/Visio to make network topology map.
* Excellent experience in DNS, DHCP, WINS, LDAP

Specialties: Corporate IT infracture including Data/Voice network, Windows domain, Linux server, enduser computer, antivirus, antispam, backup.

Experience

Tier 3 Service Assurance Engineer

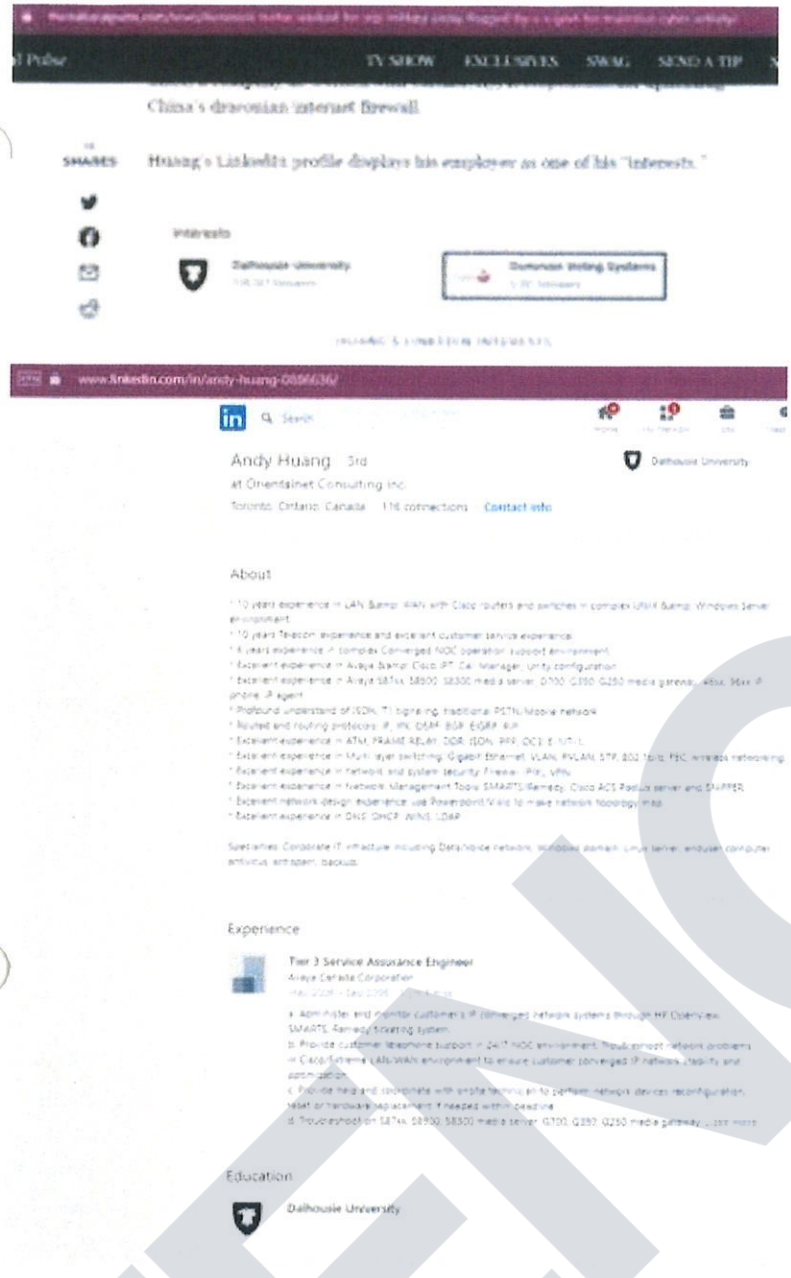
Avaya Canada Corporation

May 2006 – Sep 2009 · 3 yrs 5 mos

a. Administer and monitor customer's IP converged network systems through HP OpenView, SMARTS, Remedy ticketing system.
b. Provide customer telephone support in 24/7 NOC environment. Troubleshoot network problems in Cisco/Extreme LAN/WAN environment to ensure customer converged IP network stability and optimization.
c. Provide help and coordinate with onsite technician to perform network devices reconfiguration, reset or hardware replacement if needed within deadline
d. Troubleshoot on S87xx, S8500, S8300 media server, G700, G350, G250 media gateway, ...see more

Education

Dalhousie University



TV SHOW EXCLUSIVES SWAG SEND A TIP

China's draconian internet firewall

SHARES

Huang's LinkedIn profile displays his employer as one of his "interests."

Interests

Dalhousie University

Dominion Voting Systems

www.linkedin.com/in/andy-huang-0856636/

Search

Andy Huang 3rd

at Orientslnet Consulting Inc.

Toronto, Ontario, Canada 116 connections Contact info

Dalhousie University

About

* 10 years experience in LAN & WAN with Cisco routers and switches in complex UNIX & Windows Server environment.
* 10 years Telecom experience and excellent customer service experience.
* 6 years experience in complex Converged NOC operation support environment.
* Excellent experience in Avaya & Cisco IP, CA Manager, Unity configuration.
* Excellent experience in Avaya S87xx, S8800, S8300 media server, G700, G350, G250 media gateway, 4606, 9600 IP phone, IP agent.
* Profound understand of SDN, T1 signaling, traditional PSTN, Mobile network.
* Routed and routing protocols: IP, IPX, OSPF, BGP, EIGRP, RIP.
* Excellent experience in ATM, FRAME RELAY, DDR, ISDN, PPP, OC3, E1/T1.
* Excellent experience in Multi-layer switching: Gigabit Ethernet, VLAN, PVLAN, STP, 802.1p/q, FEC, wireless networking.
* Excellent experience in network and system security: Firewall, IPSec, VPN.
* Excellent experience in Network Management Tools: SMARTS, Remedy, Cisco ACS, Radius server and SNMPER.
* Excellent network design experience, use Powerpoint, Visio to make network topology map.
* Excellent experience in DNS, DHCP, WINS, LDAP.

Specialties: Corporate IT infrastructure including Datahouse network, windows domain, Linux server, end-user computer, antivirus, anti-spam, backups.

Experience

Tier 3 Service Assurance Engineer

Avaya Canada Corporation

a. Administer and monitor customer's IP (converged) network systems through HP OpenView, SMARTS, Remedy ticketing system.
b. Provide customer telephone support in 24x7 NOC environment. Troubleshoot network problems in Cisco Systems LAN, WAN environment to ensure customer converged IP network stability and optimization.
c. Provide help and coordinate with onsite technician to perform network devices reconfiguration, repair or hardware replacement if needed within deadline.
d. Troubleshoot on S87xx, S8800, S8300 media server, G700, G350, G250 media gateway, 4606, 9600

Education

Dalhousie University

Orientalnet Consulting Ltd. China Branch

About us	Orientalnet consulting Ltd. China trading branch is a professional manufacturer and exporter specializing in paper products. We have strong technical forces and advanced equipments. There are numerous modern and practical designs available to meet our clients' need. We also have design staff standing by to cooperate with buyers to develop new articles in accordance with their ideas, drawings and supplied samples. Furthermore, the quality, quantity and timely delivery can be fully guaranteed according to the customers' need. So OEM and ODM order are welcome. At present, we can supply 9 main series of products including gift bag, adhesive tag, picture album, gift box, sticky notes, file bag, greeting card, notebook and desk calendar. 90% of our products are exported to all over the world, especially America, Canada, Europe, Australia and middle-east countries. We are known for our honesty, efficiency, and commitment to customers. Meanwhile, in order to keep expanding our sales networks, we are continually seeking agents and distributors in countries around the world. Our mission We create value in the network of customers and suppliers. Our win-win business strategy will ensure the long-term relationship that brings success and profitability to related parties and us. Our objective Best service, best quality, the most favorable price, and the fastest delivery Your inquiries will be given our utmost attention. Please do not hesitate to contact us with the detailed specifications you need. We are looking forward to cooperating and establishing long-term business relationship with you in the soonest future.
Industry Focus	Label & Tag, Paper Crafts, Paper Box & Bag, Paper/Paperboard Packaging Products
Business Type	Trading Company
Products/Services	Paper product, gift bag, tag, picture album, gift box, label, file bag, greeting card, notebook, desk calendar
Our Markets	Worldwide
No. of Employees	5 - 10 People
Annual Sales Range(USD)	Above US$100 Million
Year Established	2001

Contact Information

Company Name	Orientalnet Consulting Ltd. China Branch
Contact Person	Ms Joyce Zeng
Company Address	Room 302, Building 4, No.25 Hexiangdong Rd, Xiamen, Fujian, China (Mainland)
Postal Code	361004
Telephone Number	+86 592 8133881
Mobile Number	
Fax Number	+86 592 5971483
Website	Orientalnet Consulting Ltd. China Branch, http://www.bizearch.com/company/Orientalnet_Consulting_Ltd_China_Branch_24063.htm

Contact Supplier / Manufacturer

GEMS-Global Election Systems-GEMS central tabulator totals the precinct vote tallies. Firmware (software) is embedded inside the hardware. Dominion acquired, Premier formerly Diebold. Dominion GEM Certificate

GEMS Software is the KEY

(GEMS owned by Dominion since 2010)

Voting Systems / Machines

Dominion* (Soros)
now owns GEMS & Sequoia

Biggest?
Most dominant?

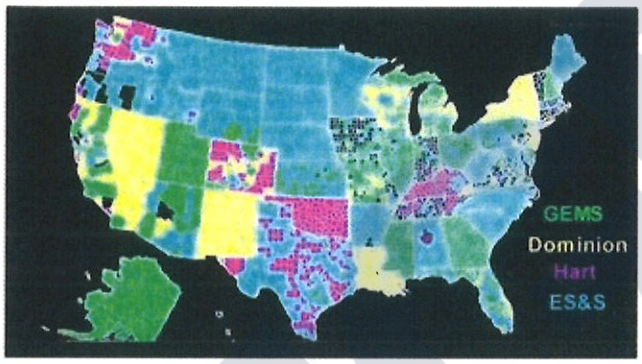
* VP of Engring Dr. Eric Coomer (admitted than many have access to voting table - no login rec.)
*Coomer formerly w/Sequoia
*What's the origin of their source code?

ES & S
Owner of GEMS 2009 - 2010
(forced to sell - anti-trust suit)
* Todd & Bob Urosevich = founders (AIS 1979)
Largest mfr of voting machines

Hart InterCivic
(2019: 80% H.I.G. Capital, 10% GL Burt -- owner now - ?? - hidden)
* Their new machines can connect to Net (illegal)
*A subsidiary is pro-Biden
*Very involved in currently contested states
Source: >>>/midnightriders/11253

Sequoia
(owned by Dominion since 2009 - 2010
*Previously owned by Smartmatic (2005 - 2006)
* code is from Venezuela
* Sold coz controversial
* Romney fam investment

Smartmatic* (Brown)
* linked to Chavez takeover in Venezuela
* Founder: Antonio Mugica
* (owned by ??)
* Software used by Sequoia - Bitza (Chavez gov)
* Made 2000 election faulty cards; thus > electronic voting
* Romney fam investment



Map Source: Fraction Magic - Detailed Vote Rigging Demonstration
Beverly Harris - https://www.youtube.com/watch?v=Fob-AGgZn44 - Oct 31, 2016

*Diebold/DESI/Premier owned GEMS until 2009, when it was sold to ES&S, then to Dominion in 2010 (due to an anti-trust suit)

**Smartmatic is not on this map because it has had a non-compete clause with Dominion not to do business within the United States
Source: https://www.potteranderson.com/delawarecase-77.html

FINDINGS SO FAR

Voting software & hardware is in the hands of a small gp of companies run by people who have worked together in the industry for years. All have been involved in voter fraud issues. Dominion seems to be the most dominant but all are highly influential & have strong ties to one another and to gov't structures at all levels plus top agencies (e.g., CISA & Homeland Security)

VERSION 4. 11-15-2020

3.1 Software/Firmware

The following software/firmware is required for the execution Dominion Assure 1.3 EAC Modification tests. This includes all supporting software such as operating systems, compilers, assemblers, application software, firmware, any applications used for burning of media, transmission of data or creation/management of databases.

3.1.1 Manufacturer Software/Firmware

The following table details the portions of the Assure 1.3 system that will be exercised in the testing of the modifications.

Table 1 – Manufacturer Software/Firmware

Application	Version
GEMS	software version 1.21.6
AV-OS PC	firmware version 1.96.14
AV-OSX	firmware version 1.2.7
AV-TSX DRE	firmware version 4.7.10
AV-TS R6 DRE	firmware version 4.7.10
ABasic script for state of Vermont	in GEMS 1.21.6

3.1.2 Additional Supporting Test Software

No additional supporting test software will be utilized in this certification test campaign.

Kamala Harris' husband, Doug Emhoff is partner at DLA Piper. Smartmatic's CEO Antonio Mugica & Lord Mark Malloch-Brown launched SGO Corp whose primary asset is the election technology & voting machine manufacturer. Sir Nigel Knowles, is Co-chairman of DLA Piper & Dir at SGO.

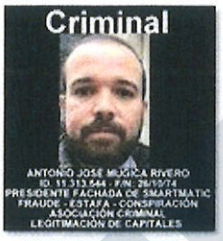
In 2014, Smartmatic CEO Antonio Mugica and British Lord Mark Malloch-Brown announced the launching of the SGO Corporation Limited

DLA PIPER

sgo

Corp Ltd
London UK

Antonio Mugica
founder and CEO of Smartmatic



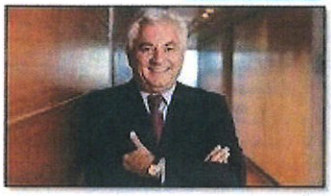
Corp Ltd
London UK

sgo

DLA PIPER

Doug Emhoff took a leave of absence from the law firm, DLA Piper, in August, after now President-elect Joe Biden, a Democrat, named Harris as his running mate. A Biden campaign representative said Emhoff will sever all ties with DLA Piper by Inauguration Day, Jan. 20, 2021.

Sir Nigel Knowles is the former global co-chairman of the law firm DLA Piper & Current Director at SGO Corp Ltd



DOMINION VOTING

Lord Mark Malloch Brown, The Soros Open Society Foundation co-founder & board Member, owns Smartmatic (Dominion Voting Systems)

Kamala Harris's Husband ???? Connections To Smartmatic & Dominion Voting Systems...
BY CLOVERCHRONICLE ON NOVEMBER 16, 2020

https://cloverchronicle.com/2020/11/15/kamala-harriss-husband-douglas-emhoff-may-have-connections-to-smartmatic-dominion-voting-systems/
https://www.biometricupdate.com/201411/smartmatic-spins-off-new-parent-company-sgo-with-british-lord
https://economictimes.indiatimes.com/news/international/world-news/vice-president-elect-kamala-harris-husband-leaves-job-at-powerhouse-law-firm-dla-piper/articleshow/79163865.cms

The link Between Dominion, Sequoia, Smartmatic, and the CCP. Sequoia Capital funded Dominion Voting Systems. Neil Shen is the Founder of Sequoia. This is the key to the connection with the Chinese Communist Party (CCP).

WORLD ECONOMIC FORUM Agenda Platforms Reports Events Videos English Sign-in

Neil Shen Nan Peng

Founding and Managing Partner, Sequoia Capital

Bachelor's degree, Shanghai Jiao Tong University; Master's degree, Yale University. Founding and Managing Partner, Sequoia Capital China. Co-Founder, Ctrip.com and Home Inns. Rotating President and Director, China Entrepreneur Forum. Chairman of the Board, Yale Leadership Center in China. Trustee, Asia Society. Vice-Chairman: Beijing Private Equity Association; Zhejiang Chamber of Commerce Shanghai. Named: to Forbes Global Midas List (2012-2015) as the highest ranking investor from China; one of China's 50 Most Influential Business Leaders in 2015, Fortune Magazine; one of 25 Most Influential Entrepreneurs in 2014, China Entrepreneur Magazine; Venture Capital Professional of the Year, AVCJ (2010); one of Top Ten Chinese Economy Leaders in 2010, 21 Century Economic Report; one of Top Ten Economic Figures in 2006, CCTV; Entrepreneur of the Year, AVCJ (2004).

Neil Shen is the Founding & Managing Partner of Sequoia Capital China. He is also a co-founder of Ctrip.com (NASDAQ: CTRP) and Home Inns (NASDAQ: HMIN).

A Chinese Bank, HSBC secures the patents pertaining to the U.S. election systems. Dominion Voting Systems entered into a "security agreement" w/ HSBC & received ownership of patents pertaining to intellectual property w/ elections, ballots, systems, cyber & internet capacities.

At this juncture, we are latching on to Sequoia Capital and for good cause. It should be noted here and importantly so, that Sequoia Capital and Sequoia Voting systems are only similar in name. They are not the same entity.

I also recommend taking a quick spin through Sequoia's website by clicking on the above image.

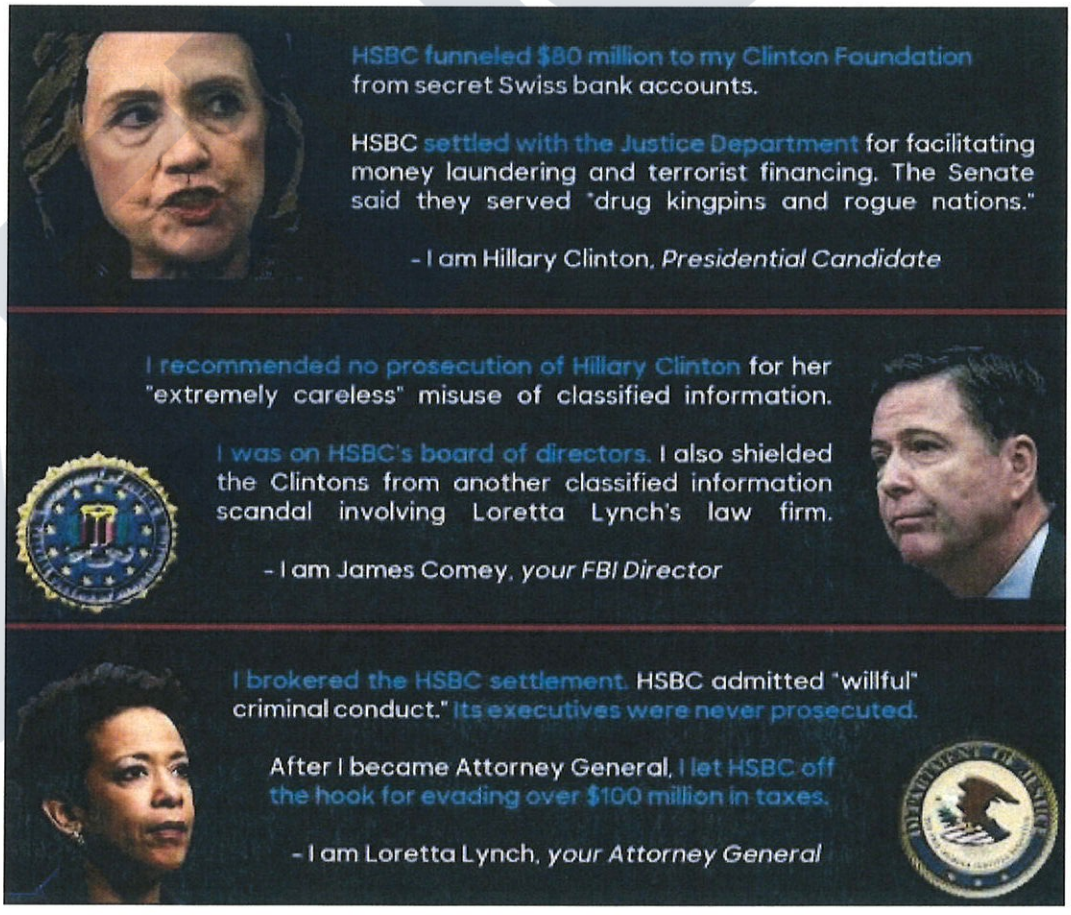
Recall here that Sequoia Capital seeded or funded Dominion Voting Systems and HSBC Toronto acquired from Dominion Voting Systems 18 patents representing the intellectual property of Dominion. Those patents all pertain to direct interfaces with the U.S. election process by means of ballots, systems and machines. Again, see the last article for details here because they are imperative to have.

A Toronto-based Chinese bank (HSBC) secures the intellectual patents pertaining to direct access to the U.S. election systems and equipment from Dominion Voting Systems. DVS is seeded by Sequoia Capital, which is affiliated with Cyberbank in the British Virgin Islands. Both Sequoia and HSBC are found in bed together with the China Online Education Group, which follows an established pattern (modus operandi) of directly linking American educators to Chinese foreign nationals for ulterior and nefarious purposes. Immediately pursuant to the stolen 2020 election, HSBC and Sequoia close out their positions on the group and whereby it ties directly to California PERS. California is an immensely corrupt state, its finances are atrocious, Gavin Newsome is the governor and his aunt and fellow resident is Nancy Pelosi. And all of that ties back to the very first article in all of this as it relates to George Soros. And we didn't talk about a mountain's worth of details in between.

At this point, I would refer you to the bank accounts and investment portfolios of Gavin Newsome and Nancy Pelosi. I wonder if either has a trust at Portcullis. I wonder if either has inroads to Cyberbank. I wonder if they hang-out with Shen? What about their connections to HSBC? How do politicians get so filthy rich on their public salaries?

James Comey was appointed to HSBC board of directors. The Massive HSBC Sandal for laundering billions for drug traffickers/arms dealers was covered up when Obama's AG Loretta Lynch struck a deal. Clintons received $81M Via HSBC Clients. HSBC-Hongkong/Shanghai Bank

https://www.wnd.com/2015/02/emerging-obama-scandal-1st-found-by-wnd-in-2012/



HSBC About HSBC Our approach Investor relations News and insight Careers Online banking

Home > News and insight > Media resources > Media releases > Former US Deputy Attorney General joins HSBC Board

30 Jan 2013

Former US Deputy Attorney General joins HSBC Board

Print Share

Media resources

Group Press Office:
+44(0) 20 7991 8096

Contact us

James Brien Comey, Jr. (52), former United States Deputy Attorney General, has been appointed a Director of HSBC Holdings plc with effect from 4 March 2013. He will be an independent non-executive Director and a member of the Financial System Vulnerabilities Committee.

Jim Comey is a Senior Research Scholar and Hertog Fellow on National Security Law at Columbia University Law School in New York. From 2010 to 2013, he was General Counsel of Bridgewater Associates, LP and, from 2005 to 2010, Senior Vice President and General Counsel of the Lockheed Martin Corporation. From 2003 to 2005, he served as United States Deputy Attorney General and was responsible for supervising the operations of the Department of Justice and chaired the President's Corporate Fraud Task Force. From 2002 to 2003, Mr. Comey

The CCP Captured U.S. by Controlling Sequoia Capital. Smartmatic acquired Sequoia Voting Systems. Smartmatic was co-founded in Venezuela. Venezuela is controlled by the CCP. Smartmatic sold Sequoia Voting Systems to Dominion and continues to use Sequoia's updated software.

Roger Piñate

President

Antonio Mugica

Chief Executive Officer

The actual controller behind Smartmatic is the former Venezuelan President Chavez. He later transferred management to the current President Maduro. While Venezuela is controlled by the CCP, Maduro is actually the CCP's bagman. In other words, Smartmatic is a company controlled by the CCP, so after its acquisition of Sequoia Voting Systems, the CCP has become the actual controller of the company. After the CCP controlled Sequoia Voting Systems, it developed and updated the voting system software for the CCP. We believe that this voting software has been completely controlled by the CCP since then.

https://en.wikipedia.org/wiki/Smartmatic

No. 1

Neil Shen

Sequoia Capital China

Founding Partner

The Carlyle Group & The CCP: In 2018, Dominion was acquired by David Rubenstein, founder of The Carlyle Group. The Carlyle Group is the largest global investment company in China. The Carlyle Group ties former George HW Bush & top globalist politicians Worldwide.

CCP Controls Dominion: The controller of Dominion is the Carlyle Group, which is inextricably linked to the CCP. The CCP gained control of Dominion by opening up resource companies to the Carlyle Group. Controlling the votes of Americans, Politicians and the U.S. itself.

Sequoia Capital

founded by Don Valentine in 1972 in California

In 1984, Sequoia purchased the voting machine business of AVM Corporation (the former Automatic Voting Machine Corporation) and established:

Sequoia Voting Systems

In 2005 acquired by:

Smartmatic

Founded In 1997 by three engineers, Antonio Mugica, Alfredo José Anzola and Roger Piñate, in Venezuela,and was officially incorporated in 2000 in Delaware

In 2005, Shen Nanpeng and Sequoia Capital jointly established Sequoia Capital China Fund

In 2010, Smartmatic sold the Sequoia Voting Systems to:

Dominion

was founded in 2002 in Toronto, Ontario, Canada, the company sells electronic voting hardware and software, including voting machines and tabulators, in the United States and Canada.

The Carlyle Group is the biggest shareholder of Dominion.

In 2018, purchased by:

Staple Street Capital

Owned by David Mark Rubenstein who is also the founder of The Carlyle Group, the shareholder of the company behind Dominion..

The Carlyle Group

was founded in 1987 as an investment banking boutique, and has wide business relation with Chinese companies under Jiang Zemin family control

Conclusion:

Dominion

Is controlled by CCP company

We believe this is an exchange of interests between the CCP and Sequoia Capital. Sequoia Capital helps the CCP control Sequoia Voting Systems to realize its ambition to manipulate the American political arena, and the CCP pays it back through the exchange of capital interests.

In 2010, Smartmatic sold Sequoia Voting Systems to Dominion Voting Systems. Dominion continues to use Sequoia's updated software.

HSBC received ownership of patents to intellectual property of elections, ballots, systems, cyber & internet capacities. Patent Agreement

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame
050500/0236

Execution date
Sep 25, 2019

Date recorded
Sep 26, 2019

Conveyance
SECURITY AGREEMENT

Assignors
DOMINION VOTING SYSTEMS CORPORATION

Correspondent
CHAPMAN & CUTLER LLP
1270 AVENUE OF THE AMERICAS, 30TH FLOOR
ATTN: SOREN SCHWARTZ
NEW YORK, NY 10020

Assignee
HSBC BANK CANADA, AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET
TORONTO M5J 1S9
CANADA

Properties (18)

Patent	Publication	Application	PCT
8844813	20130306724	13476836	
8913787	20130301873	13470091	
9202113	20150071501	14539684	
8195505	20050247783	11121997	
9870666	20120232963	13463536	
9710988	20120259680	13525187	
9870667	20120259681	13525208	
7111782	20040238632	10811969	
7422151	20070012767	11526028	
D599131		29324281	

505692196 09/26/2019

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT5739006

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	SECURITY AGREEMENT

CONVEYING PARTY DATA

Name	Execution Date
DOMINION VOTING SYSTEMS CORPORATION	09/25/2019

RECEIVING PARTY DATA

Name:	HSBC BANK CANADA, AS COLLATERAL AGENT
Street Address:	4TH FLOOR, 70 YORK STREET
City:	TORONTO
State/Country:	CANADA
Postal Code:	M5J 1S9

PROPERTY NUMBERS Total: 18

Property Type	Number
Patent Number:	8844813
Patent Number:	8913787
Patent Number:	9202113
Patent Number:	8195505
Patent Number:	9870666
Patent Number:	9710988
Patent Number:	9870667
Patent Number:	7111782
Patent Number:	7422151
Patent Number:	D599131
Patent Number:	D521050
Patent Number:	D515619
Patent Number:	D521051
Patent Number:	D537469
Patent Number:	8714450
Patent Number:	8910865
Patent Number:	8864026
Patent Number:	8876002

Fax Number:
Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.
Phone: 212-655-3327
Email: sschwartz@chapman.com
Correspondent Name: CHAPMAN & CUTLER LLP
Address Line 1: 1270 AVENUE OF THE AMERICAS, 30TH FLOOR
Address Line 2: ATTN: SOREN SCHWARTZ
Address Line 4: NEW YORK, NEW YORK 10020

NAME OF SUBMITTER:	SOREN SCHWARTZ
SIGNATURE:	/Soren Schwartz/
DATE SIGNED:	09/26/2019

Total Attachments: 5
source=Dominion - Patent Recordation Form#page1.tif
source=Dominion - Patent Recordation Form#page2.tif
source=Dominion - Patent Recordation Form#page3.tif
source=Dominion - Patent Recordation Form#page4.tif
source=Dominion - Patent Recordation Form#page5.tif

Communist People's Republic of China financially captured Collateral of Dominion Voting Systems, Machines & Security Software Applications. Dominion's financial collateral owner is HSBC the Hongkong Shanghai Bank of CHINA-Assigned 18 different Patents.

U.S. Patents & Applications

Title	SERIAL #	FILED DATE	PATENT NO.	ISSUE DATE	STATUS
Electronic Correction of Voter-Marked Paper Ballot	13/476,836	5/21/2012	8,844,813	9/30/2014	Issued
Ballot Adjudication in Voting Systems Utilizing Ballot Images	13/470,091	5/11/2012	8,913,787	12/16/2014	Issued
Ballot Adjudication in Voting Systems Utilizing Ballot Images (continuation of U.S. Patent 8913787)	14/539,684	11/12/2014	9,202,113	12/1/2015	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	11/121,997	5/5/2005	8,195,505	6/5/2012	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/463,536	5/3/2012	9,870,666	1/16/2018	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/525,187	6/15/2012	9,710,988	7/18/2017	Issued
System, Method and Computer Program for Vote Tabulation with an Electronic Audit Trail	13/525,208	6/15/2012	9,870,667	1/16/2018	Issued
Systems and Methods for Providing Security in a Voting Machine	10/811,969	3/30/2004	7,111,782	9/26/2006	Issued
Systems and Methods for Providing Security in a Voting Machine	11/526,028	9/25/2006	7,422,151	9/9/2008	Issued
Voting Booth	29/324,281	9/10/2008	D599,131	9/1/2009	Issued
Voting Terminal and Stand	29/209,554	7/15/2004	D521,050	5/16/2006	Issued
Pair of Enclosure Doors	29/209,579	7/15/2004	D515,619	2/21/2006	Issued
Voting Terminal	29/209,556	7/15/2004	D521,051	5/16/2006	Issued
Voting Terminal and Keypad	29/254,483	2/23/2006	D537,469	2/27/2007	Issued
Systems and Methods for Transactional Ballot Processing, and Ballot Auditing	13/092,600	4/22/2011	8,714,450	5/6/2014	Issued
Ballot Level Security Features for Optical Scan Voting Machine Capable of Ballot Image Processing, Secure Ballot Printing, and Ballot Layout Authentication and Verification	13/092,599	4/22/2011	8,910,865	12/16/2014	Issued
Ballot Image Processing System and Method for Voting Machines	13/092,606	4/22/2011	8,864,026	10/21/2014	Issued
Systems for Configuring Voting Machines, Docking Device for Voting Machines, Warehouse Support and Asset Tracking of Voting Machines	13/092,604	4/22/2011	8,876,002	11/4/2014	Issued

Ownership of the above-referenced patents has been assigned to Dominion Voting Systems Corporation.

Canadian Patent Application

Title	APPLICATION #	FILED DATE	STATUS
SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL	2466466	5/5/2004	Pending

Dominion Voting Systems is listed in the Canadian Patent Office records as the current owner of record for the above-referenced patent application, but this application is to be assigned to Dominion Voting Systems Corporation post-Closing pursuant to the Undertaking.

U.S. Registered Trademarks

Trademark	Serial #	File Date	Reg #	Reg Date	Status	Class
	85407877	Aug-25-2011	4174339	Jul-17-2012	Registered	35 37 40 41
DOMINION VOTING	85407870	Aug-25-2011	4174338	Jul-17-2012	Registered	9 35 37 40 41
DEMOCRACY SUITE	85407749	Aug-25-2011	4153203	Jun-5-2012	Registered	9
IMAGECAST	85407735	Aug-25-2011	4131899	Apr-24-2012	Registered	9
AUDITMARK	85407731	Aug-25-2011	4269144	Jan-1-2013	Registered	9
ASSURE	78440857	Jun-24-2004	3080674	Apr-11-2006	Registered	9
AVC ADVANTAGE	73755922	Sep-30-1988	1537309	May-2-1989	Registered	9

Eric Coomer is one of the Inventors of Dominions Voting Security Features. Dominion Voting Systems Patents: Security, System & Methods:
Assignors: DOMINION VOTING SYSTEMS
Assignee: HSBC
Patent Assignment 050500/0236 SECURITY AGREEMENT

https://assignment.uspto.gov/patent/index.html#/patent/search/resultAssignment?id=50500-236

Patent assignment 050500/0236

SECURITY AGREEMENT

Date recorded	Reel/frame	Pages
Sep 26, 2019	050500/0236	7

Assignors	Execution date
DOMINION VOTING SYSTEMS CORPORATION	Sep 25, 2019

Assignee	Correspondent
HSBC BANK CANADA, AS COLLATERAL AGENT 4TH FLOOR, 70 YORK STREET TORONTO M5J 1S9 CANADA	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020

Properties (18 total)

Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN POULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC		
8195505 Jun 5, 2012	20050247783 Nov 10, 2005	11121997 May 5, 2005
3. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7422151 Sep 9, 2008	20070012767 Jan 18, 2007	11526028 Sep 25, 2006
4. BALLOT LEVEL SECURITY FEATURES FOR OPTICAL SCAN VOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION Inventors: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN		

Eric Coomer is one of the Inventors of Dominions Voting Security Features.

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

View all

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function--the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date recorded	Pages
050500/0236	Sep 25, 2019	Sep 26, 2019	7

Conveyance

SECURITY AGREEMENT

Assignors	Correspondent	Attorney docket
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020	

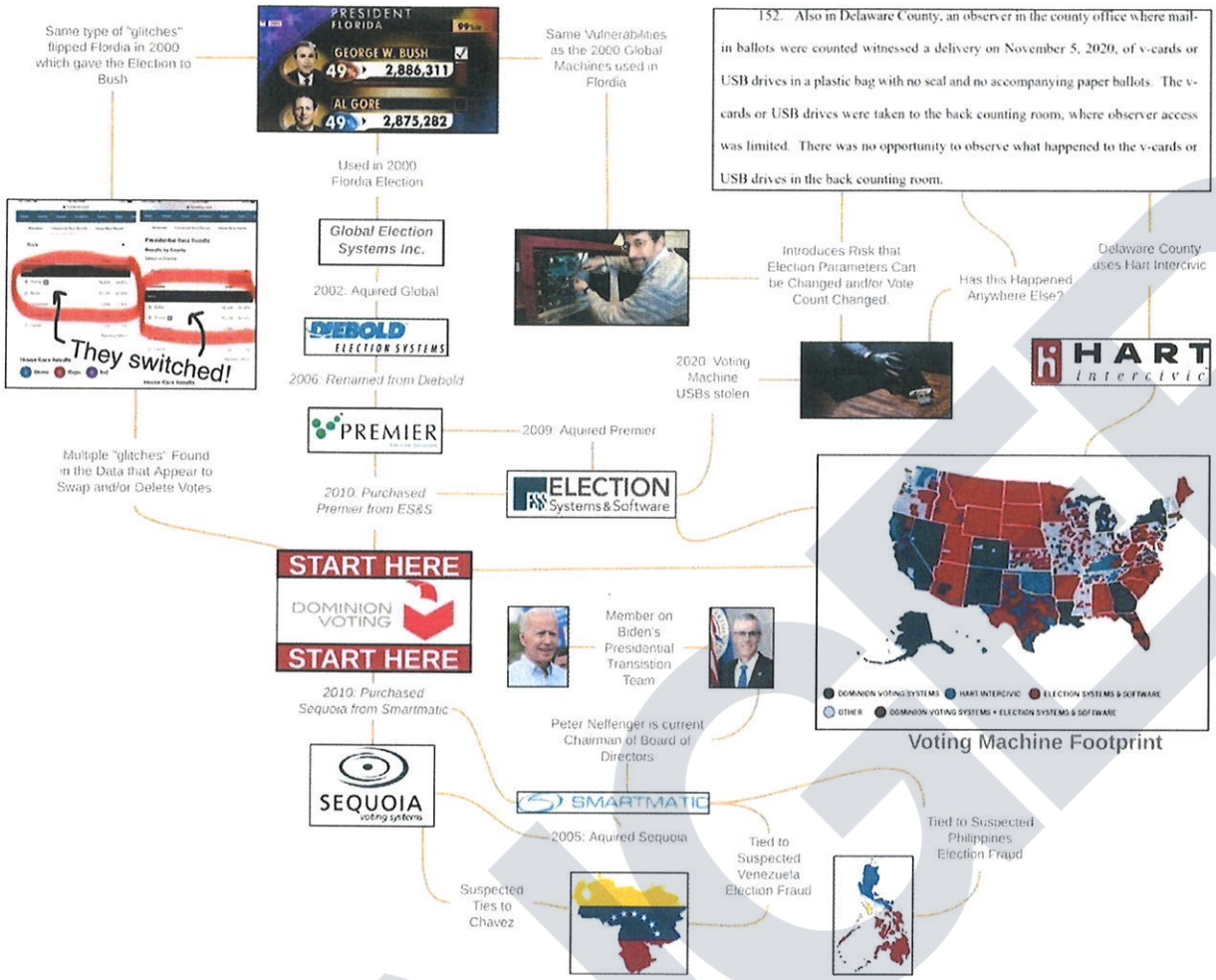
Assignee

HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA



Dominion's parent company Staple Street Capital

Owners of Dominion Voting systems, many of their leadership comes from Cerberus Capital management, from their Vice President to their Managing Director. Cerberus capital owns Remington, Bushmaster and others. This is mentioned because of the effects of the uncertainty during the pandemic and the weapons sales in the United states in regards to their profit for 2020.

Staple Street Capital has 7 current team members, including Senior Associate **Daniel Franklin**.

Daniel Franklin
Senior Associate

Hootan Yaghoobzadeh
Managing Director

Jeffrey D Hyslop
Vice President

Stephen D Owens
Managing Director & Founder

Andre Ohnona
Vice President

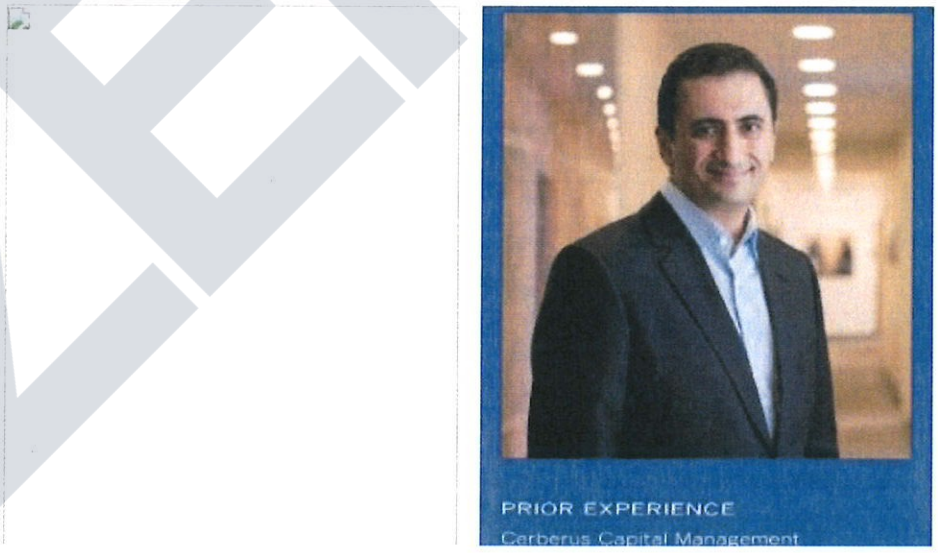
Dylan Lam
Associate

Scott Zhu
Vice President

Who owns the Dominion Voting Systems?

July 16, 2018 Dominion Voting Systems ("Dominion Voting") announces that it has been acquired by its management team and Staple Street Capital.

Staple Street Capital is a private equity firm founded in 2009 based in New York.The co-founders Stephen D. Owens and Hootan Yaghoobzadeh are veterans of The Carlyle Group and Cerberus Capital Management, also the Board members of Dominion Voting. The official website of Staple Street Capital has deleted the team introduction.



With staple street capital's ownership of Dominion, Dominion would have been included in the buy out or Staple street when UBS bought them in 2019 for 400 Million Dollars US.

The Securities and Exchange Commission has not necessarily reviewed the information in this filing and has not determined if it is accurate and complete.
The reader should not assume that the information is accurate and complete.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM D

Notice of Exempt Offering of Securities

OMB APPROVAL	
OMB Number:	3235-0076
Estimated average burden hours per response:	4.00

1. Issuer's Identity

CIK (Filer ID Number)
0001827586

Previous Names [X] None

Name of Issuer
STAPLE STREET CAPITAL III, L.P.

Jurisdiction of Incorporation/Organization
DELAWARE

Year of Incorporation/Organization
[ ] Over Five Years Ago
[X] Within Last Five Years (Specify Year) 2020
[ ] Yet to Be Formed

Entity Type
[ ] Corporation
[X] Limited Partnership
[ ] Limited Liability Company
[ ] General Partnership
[ ] Business Trust
[ ] Other (Specify)

2. Principal Place of Business and Contact Information

Name of Issuer
STAPLE STREET CAPITAL III, L.P.

Street Address 1
1290 AVENUE OF THE AMERICAS, 10TH FLOOR

Street Address 2

City
NEW YORK

State/Province/Country
NEW YORK

ZIP/PostalCode
10104

Phone Number of Issuer
(212) 613-3100

3. Related Persons

3. Related Persons

Last Name
OWENS

First Name
STEPHEN

Middle Name
D

Street Address 1
1290 AVENUE OF THE AMERICAS, 10TH FLOOR

Street Address 2

City
NEW YORK

State/Province/Country
NEW YORK

ZIP/PostalCode
10104

Relationship: [X] Executive Officer [ ] Director [X] Promoter

Clarification of Response (if Necessary)

Last Name
YAGHOOBZADEH

First Name
HOOTAN

Middle Name

Street Address 1
1290 AVENUE OF THE AMERICAS, 10TH FLOOR

Street Address 2

City
NEW YORK

State/Province/Country
NEW YORK

ZIP/PostalCode
10104

Relationship: [X] Executive Officer [ ] Director [X] Promoter

Clarification of Response (if Necessary)

4. Industry Group

[ ] Agriculture
Banking & Financial Services
[ ] Commercial Banking
[ ] Insurance
[ ] Investing
[ ] Investment Banking
[X] Pooled Investment Fund
[ ] Hedge Fund
[X] Private Equity Fund
[ ] Venture Capital Fund
[ ] Other Investment Fund
Is the issuer registered as an investment company under the Investment Company Act of 1940?
[ ] Yes [X] No
[ ] Other Banking & Financial Services
[ ] Business Services
Energy
[ ] Coal Mining
[ ] Electric Utilities
[ ] Energy Conservation
[ ] Environmental Services
[ ] Oil & Gas
[ ] Other Energy
Health Care
[ ] Biotechnology
[ ] Health Insurance
[ ] Hospitals & Physicians
[ ] Pharmaceuticals
[ ] Other Health Care
[ ] Manufacturing
Real Estate
[ ] Commercial
[ ] Construction
[ ] REITS & Finance
[ ] Residential
[ ] Other Real Estate
[ ] Retailing
[ ] Restaurants
Technology
[ ] Computers
[ ] Telecommunications
[ ] Other Technology
Travel
[ ] Airlines & Airports
[ ] Lodging & Conventions
[ ] Tourism & Travel Services
[ ] Other Travel
[ ] Other

5. Issuer Size

Revenue Range	OR	Aggregate Net Asset Value Range
[ ] No Revenues		[ ] No Aggregate Net Asset Value
[ ] $1 - $1,000,000		[ ] $1 - $5,000,000
[ ] $1,000,001 - $5,000,000		[ ] $5,000,001 - $25,000,000
[ ] $5,000,001 - $25,000,000		[ ] $25,000,001 - $50,000,000
[ ] $25,000,001 - $100,000,000		[ ] $50,000,001 - $100,000,000
[ ] Over $100,000,000		[ ] Over $100,000,000
[X] Decline to Disclose		[ ] Decline to Disclose
[ ] Not Applicable		[ ] Not Applicable

6. Federal Exemption(s) and Exclusion(s) Claimed (select all that apply)

	[X] Investment Company Act Section 3(c)	
[ ] Rule 504(b)(1) (not (i), (ii) or (iii))	[X] Section 3(c)(1)	[ ] Section 3(c)(9)
[ ] Rule 504 (b)(1)(i)	[ ] Section 3(c)(2)	[ ] Section 3(c)(10)
[ ] Rule 504 (b)(1)(ii)	[ ] Section 3(c)(3)	[ ] Section 3(c)(11)
[ ] Rule 504 (b)(1)(iii)	[ ] Section 3(c)(4)	[ ] Section 3(c)(12)
[X] Rule 506(b)	[ ] Section 3(c)(5)	[ ] Section 3(c)(13)
[ ] Rule 506(c)	[ ] Section 3(c)(6)	[ ] Section 3(c)(14)
[ ] Securities Act Section 4(a)(5)	[X] Section 3(c)(7)	

7. Type of Filing

[X] New Notice Date of First Sale [X] First Sale Yet to Occur
[ ] Amendment

8. Duration of Offering

Does the Issuer intend this offering to last more than one year? [ ] Yes [X] No

9. Type(s) of Securities Offered (select all that apply)

[X] Equity	[X] Pooled Investment Fund Interests
[ ] Debt	[ ] Tenant-in-Common Securities
[ ] Option, Warrant or Other Right to Acquire Another Security	[ ] Mineral Property Securities
[ ] Security to be Acquired Upon Exercise of Option, Warrant or Other Right to Acquire Security	[ ] Other (describe)

10. Business Combination Transaction

Is this offering being made in connection with a business combination transaction, such as a merger, acquisition or exchange offer? [ ] Yes [X] No

10. Business Combination Transaction

Is this offering being made in connection with a business combination transaction, such as a merger, acquisition or exchange offer? [ ] Yes [X] No

Clarification of Response (if Necessary):

11. Minimum Investment

Minimum investment accepted from any outside investor $0 USD

12. Sales Compensation

Recipient
UBS SECURITIES LLC

Recipient CRD Number [ ] None
7654

(Associated) Broker or Dealer [X] None
None

(Associated) Broker or Dealer CRD Number [X] None
None

Street Address 1
1285 AVENUE OF THE AMERICAS

Street Address 2

City
NEW YORK

State/Province/Country
NEW YORK

ZIP/Postal Code
10019

State(s) of Solicitation (select all that apply)
Check "All States" or check individual States [X] All States

[ ] Foreign/non-US

13. Offering and Sales Amounts

Total Offering Amount	$400,000,000 USD	or [ ] Indefinite
Total Amount Sold	$0 USD	
Total Remaining to be Sold	$400,000,000 USD	or [ ] Indefinite

Clarification of Response (if Necessary):

The general partner of the Issuer reserves the right to offer a greater or lesser amount of limited partner interests. The Total Offering Amount and Total Remaining to be Sold are aggregated together with the Issuer and its related parallel fund.

14. Investors

[ ] Select if securities in the offering have been or may be sold to persons who do not qualify as accredited investors, and enter the number of such non-accredited investors who already have invested in the

14. Investors

☐ Select if securities in the offering have been or may be sold to persons who do not qualify as accredited investors, and enter the number of such non-accredited investors who already have invested in the offering.

Regardless of whether securities in the offering have been or may be sold to persons who do not qualify as accredited investors, enter the total number of investors who already have invested in the offering: 0

15. Sales Commissions & Finder's Fees Expenses

Provide separately the amounts of sales commissions and finders fees expenses, if any. If the amount of an expenditure is not known, provide an estimate and check the box next to the amount.

Sales Commissions $0 USD [X] Estimate

Finders' Fees $0 USD [X] Estimate

Clarification of Response (if Necessary):

Placement agent fees to be paid based upon a fee schedule. Such fees are offset dollar-for-dollar against the management fees payable by the Issuer.

16. Use of Proceeds

Provide the amount of the gross proceeds of the offering that has been or is proposed to be used for payments to any of the persons required to be named as executive officers, directors or promoters in response to Item 3 above. If the amount is unknown, provide an estimate and check the box next to the amount.

$0 USD [X] Estimate

Clarification of Response (if Necessary):

The general partner is entitled to a performance allocation. The investment manager is entitled to a management fee. The performance allocation and management fees are fully disclosed in the Issuer's confidential offering materials.

Signature and Submission

Please verify the information you have entered and review the Terms of Submission below before signing and clicking SUBMIT below to file this notice.

Terms of Submission

In submitting this notice, each issuer named above is:

- Notifying the SEC and/or each State in which this notice is filed of the offering of securities described and undertaking to furnish them, upon written request, in the accordance with applicable law, the information furnished to offerees.*
- Irrevocably appointing each of the Secretary of the SEC and, the Securities Administrator or other legally designated officer of the State in which the issuer maintains its principal place of business and any State in which this notice is filed, as its agents for service of process, and agreeing that these persons may accept service on its behalf, of any notice, process or pleading, and further agreeing that such service may be made by registered or certified mail, in any Federal or state action, administrative proceeding, or arbitration brought against the issuer in any place subject to the jurisdiction of the United States, if the action, proceeding or arbitration (a) arises out of any activity in connection with the offering of securities that is the subject of this notice, and (b) is founded, directly or indirectly, upon the provisions of: (i) the Securities Act of 1933, the Securities Exchange Act of 1934, the Trust Indenture Act of 1939, the Investment Company Act of 1940, or the Investment Advisers Act of 1940, or any rule or regulation under any of these statutes, or (ii) the laws of the State in which the issuer maintains its principal place of business or any State in which this notice is filed.
- Certifying that, if the issuer is claiming a Regulation D exemption for the offering, the issuer is not disqualified from relying on Rule 504 or Rule 506 for one of the reasons stated in Rule 504(b)(3) or Rule 506(d).

Each Issuer identified above has read this notice, knows the contents to be true, and has duly caused this notice to be signed on its behalf by the undersigned duly authorized person.

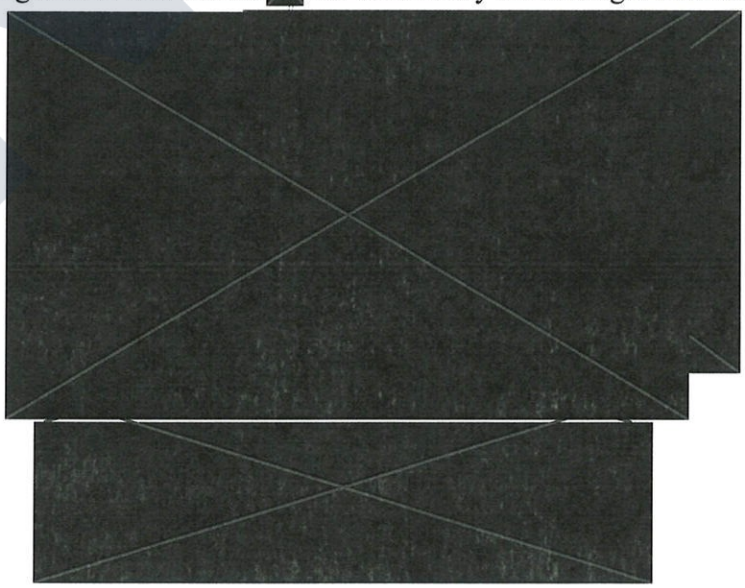
For signature, type in the signer's name or other letters or characters adopted or authorized as the signer's signature.

Issuer	Signature	Name of Signer	Title	Date
STAPLE STREET CAPITAL III, L.P.	/S/ HOOTAN YAGHOOBZADEH	HOOTAN YAGHOOBZADEH	MANAGER OF THE GP OF THE GP OF THE ISSUER	2020-10-08

Persons who respond to the collection of information contained in this form are not required to respond unless the form displays a currently valid OMB number.

* This undertaking does not affect any limits Section 102(a) of the National Securities Markets Improvement Act of 1996 ("NSMIA") [Pub. L. No. 104-290, 110 Stat. 3416 (Oct. 11, 1996)] imposes on the ability of States to require information. As a result, if the securities that are the subject of this Form D are "covered securities" for purposes of NSMIA, whether in all instances or due to the nature of the offering that is the subject of this Form D, States cannot routinely require offering materials under this undertaking or otherwise and can require offering materials only to the extent NSMIA permits them to do so under NSMIA's preservation of their anti-fraud authority.

I declare under penalty of perjury that the forgoing is true and correc[redacted] the best of my knowledge. Executed this November 23th, 2020.

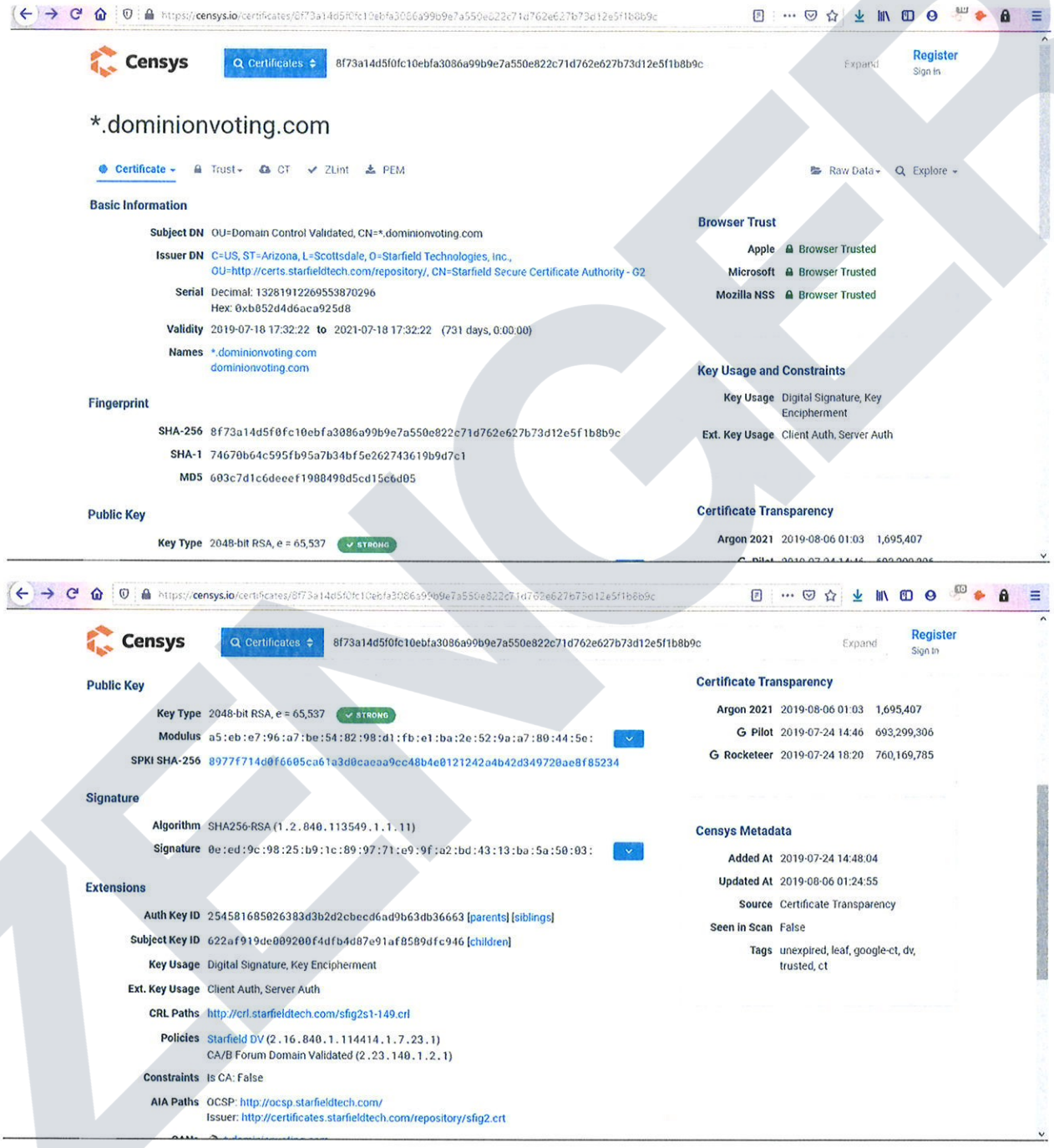


Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], make the following declaration.

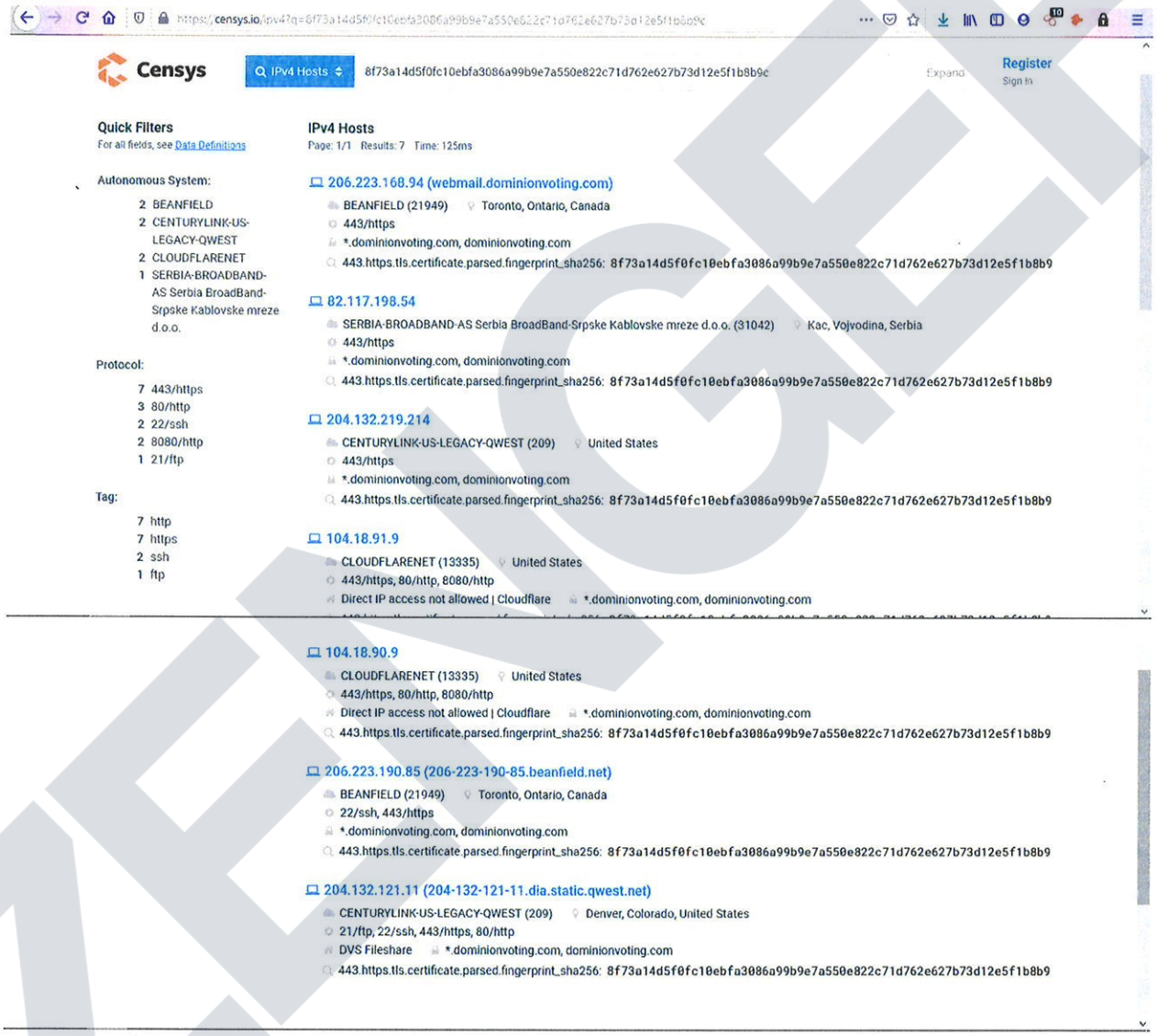
1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. [redacted]
3. I am a US citizen and I reside at [redacted] in the United States of America.
4. It can be seen using open source methodology that the SSL certificates from *.dominionvoting.com were registered on the 24th of July 2019. This SSL certificate were used multiple times from locations ranging from Canada, Serbia, and the United States. These images verify that Dominion systems were connected to foreign systems across the globe. Also seen is that the SSL certificate is used for the email server that was the same for the secure HTTP connections.

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c



All share:

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9



Email ip address

206.223.168.94

Serbian ip address

82.117.198.54

Dominion site

204.132.219.214

Cloudflare link

104.18.91.9

Canadian ip address

206.223.190.85

Denver ip address

204.132.121.11

Page: 1/1 Results: 7 Time: 155ms

206.223.168.94 (webmail.dominionvoting.com)

BEANFIELD (21949) Toronto, Ontario, Canada
443/https
*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

82.117.198.54

SERBIA-BROADBAND-AS Serbia BroadBand-Srpske Kablovske mreze d.o.o. (31042) Kac, Vojvodina, Serbia
443/https
*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

204.132.219.214

CENTURYLINK-US-LEGACY-QWEST (209) United States
443/https
*.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.91.9

CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

104.18.90.9

CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

206.223.190.85 (206-223-190-85.beanfield.net)

BEANFIELD (21949) Toronto, Ontario, Canada
22/ssh, 443/https
*.dominionvoting.com, dominionvoting.com

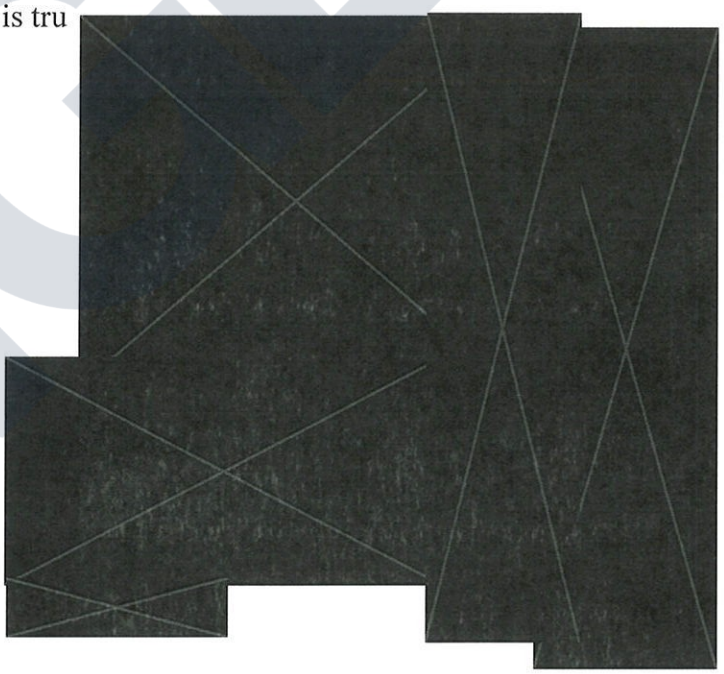
443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

204.132.121.11 (204-132-121-11.dia.static.qwest.net)

CENTURYLINK-US-LEGACY-QWEST (209) Denver, Colorado, United States
21/ftp, 22/ssh, 443/https, 80/http
DVS Fileshare *.dominionvoting.com, dominionvoting.com

443.https.tls.certificate.parsed.fingerprint_sha256:
8f73a14d5f0fc10ebfa3086a99b9e7a550e822c71d762e627b73d12e5f1b8b9c

I declare under penalty of perjury that the forgoing is tru
knowledge. Executed this December 16, 2020.



Foreign Ties and Vulnerabilities

Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], make the following declaration.

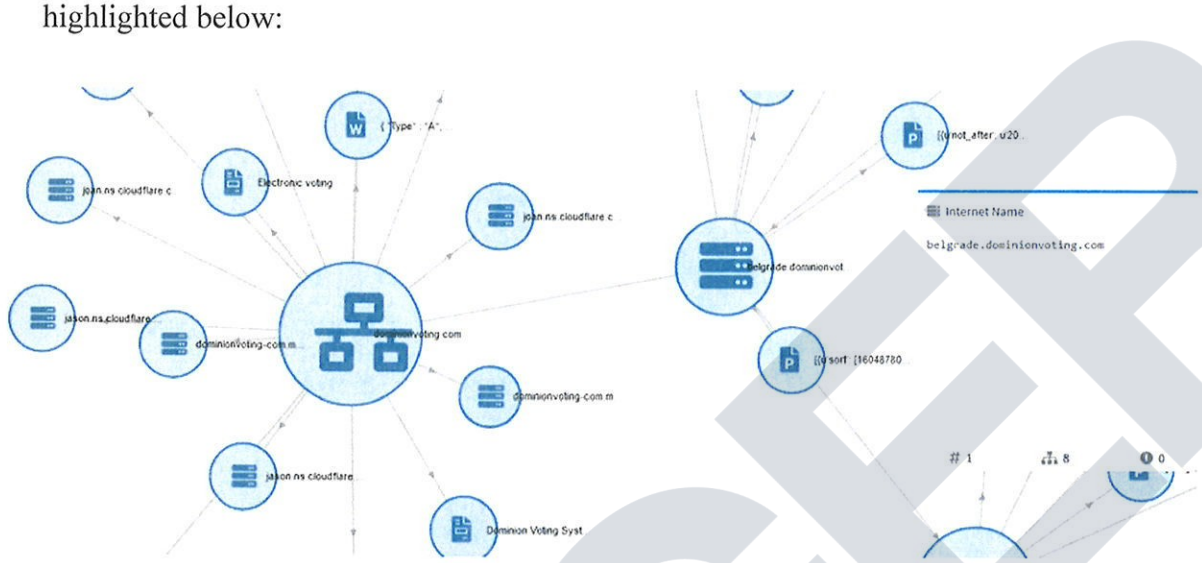
1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. [redacted]
3. I am a US citizen and I reside[redacted]in the United States of America.
4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,

7. A public network scan of Dominionvoting.com on 2020-11-08 revealed the following inter-relationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:

```
Array
(
    [id] => 544167324
    [luser] => ian.macvicar
    [domain] => dominionvoting.com
    [password] => jamley
)

7
Array
(
    [id] => 599400504
    [luser] => jelena.tanaskovic
    [domain] => dominionvoting.com
```

8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:



robtex.com/dns-lookup/dominionvoting.com

8 results shown.

IP numbers of the name servers
2400:cb00:2049:1::adf5:3bb3
2606:4700:50::adf5:3aad
2803:f800:50::6ca2:c0ad
2803:f800:50::6ca2:c1b3
2a06:98c1:50::ac40:20ad
108.162.192.173
108.162.193.179

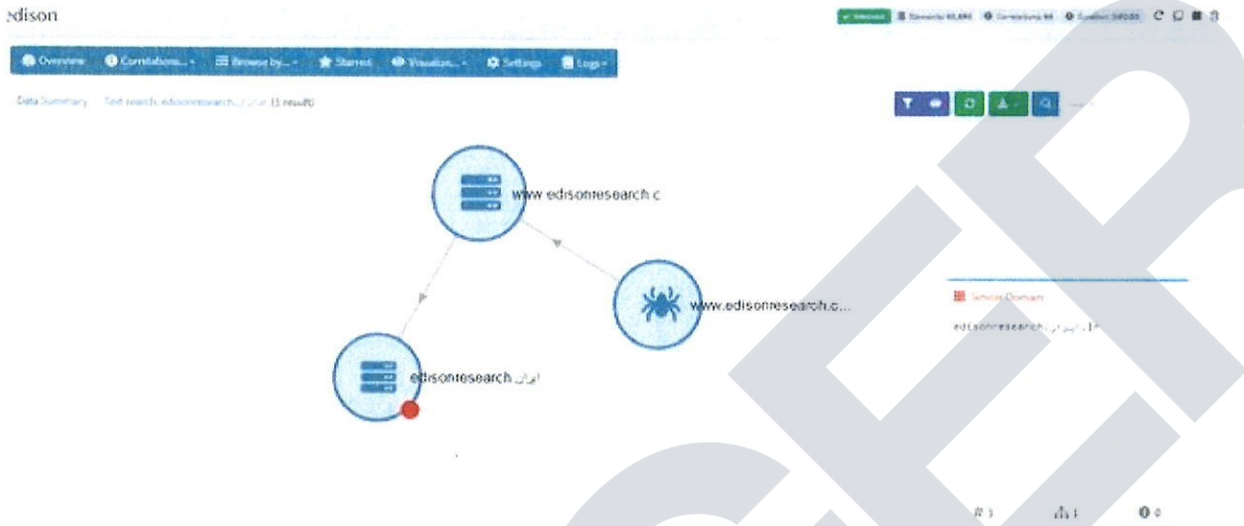
Subdomains/Hostnames
Domains or hostnames one step under this dom
barracuda.**dominionvoting**.com
belgrade.**dominionvoting**.com
webmail.**dominionvoting**.com
www.**dominionvoting**.com
4 results shown.

9. A cursory search on LinkedIn of "dominion voting" on 11/19/2020 confirms the numerous employees in Serbia:

Vukašin Đorđević • 3rd
Software Developer at Dominion Voting Systems
Serbia

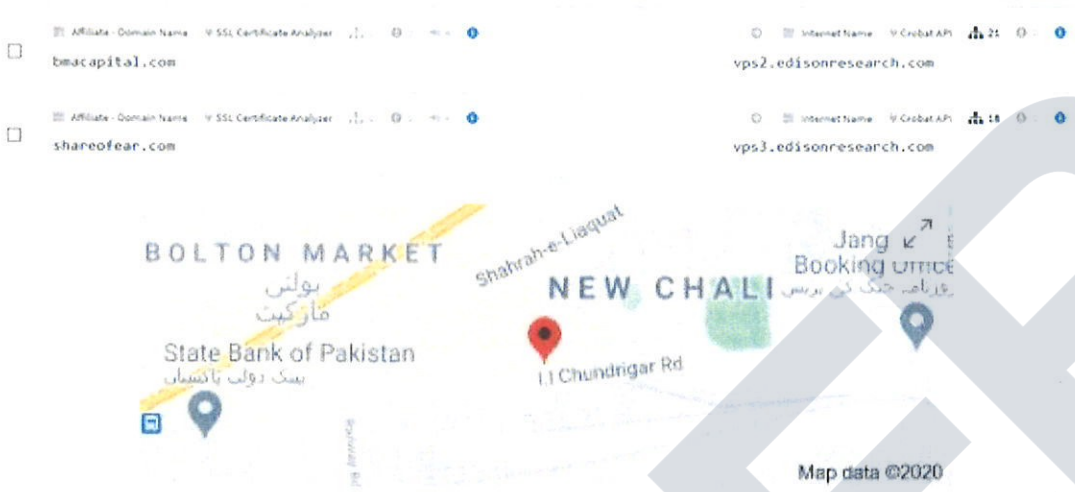
Edvan Sabanovic • 3rd
Senior Full-stack Web Developer
Belgrade, Serbia
Past: Senior Web Developer at **Dominion Voting** Systems

10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:

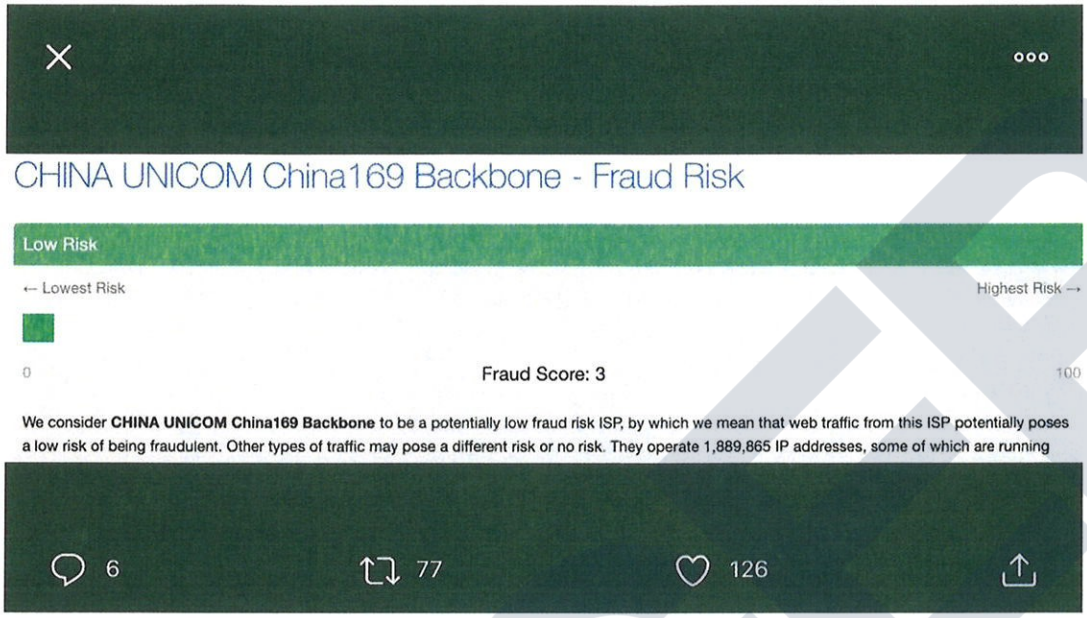


Inputting the Iranian IP into Robtex confirms the direct connection into the "edisonresearch" host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.

A deeper search of the ownership of Edison Research "edisonresearch.com" shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the "vps" at the start of the internet name:



There are also many more examples, including access of the network from China. The records of China accessing the server are reliable.



Domain Name: dominionvotingsystems.com
Registry Domain ID: 2530599738_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-05-26T15:48:58Z
Creation Date: 2020-05-26T15:48:57Z
Registrar Registration Expiration Date: 2021-05-26T15:48:57Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Hunan
Registrant Country: CN
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com
Name Server: NS1.DNS.COM
Name Server: NS2.DNS.COM
DNSSEC: unsigned

Overview - dominionvotingsystems.com

DNS Records 4

Type	Value	OSH	Security score
A	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	15
NS	ns1.dns.com		
	27.152.186.193 - AS133776 - Quanzhou	9	100
	119.167.180.131 - AS4837 - CHINA UNICOM China169 Bac...	8	100
	218.98.111.202 - AS21859 - ZNET	14	100
NS	ns2.dns.com		
	183.253.57.193 - AS9808 - Guangdong Mobile Communic...	6	100
	121.12.104.65 - AS134763 - CHINANET Guangdong provin...	4	100
SOA	ns1.dns.com		
	dnsadmin.dns.com		

View all DNS Records

Domains with same A records - dominionvotingsystems.com

1 Domains with same A records

Domain	Site Title	Alexa rank	DNS A	OSH	DNS CNAME
boao@ubal.com	--	--	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	--

CVE - dominionvotingsystems.com

22 CVE

Id	Base Score	Severity	Vector	Source	Description
CVE-2014-2653	2.6	LOW	AV:N/AC:H/Au:N/C:N/I:P/A:N	45.195.162.194	ssh/key.c in the ssh client allows remote SSH servers to bypass a hostkey.revoked restriction via a crafted key, or an empty file, which...
CVE-2016-6564	6.9	MEDIUM	AV:L/AC:M/Au:N/C:C/I:C/A:C	45.195.162.194	Use-after-free vulnerability in the sess_teardown function in sshd in OpenSSH before 7.3 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpected early MONITOR_REQ_PAM_INIT_CTX request.
CVE-2016-1908	7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	45.195.162.194	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.
CVE-2016-10010	6.9	MEDIUM	AV:L/AC:M/Au:N/C:C/I:C/A:C	45.195.162.194	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via crafted session... related to sshmonitor.c
CVE-2016-6515	7.8	HIGH	AV:N/AC:L/Au:N/C:N/I:N/A:C	45.195.162.194	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2015-5600	8.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:C	45.195.162.194	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption, resource leakage, and duplicate list in the sshd -oChallengeResponseAuthentication=yes option, as demonstrated by a modified client that provides a different password for each password prompt, aka SSHD-CVE-2015-5600.
CVE-2015-5352	4.3	LOW	AV:L/AC:M/Au:N/C:N/I:P/A:N	45.195.162.194	The x11_open_helper function in channels.c in ssh in OpenSSH before 7.0 on non-OpenBSD platforms accepts X connections after 120 seconds by default, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by guessing the DISPLAY value of 10.0. NOTE: the vendor reports that this "hardening feature" has "never shown itself to be useful," and disables it by default in OpenSSH 7.0 and later.
CVE-2016-10012	7.2	HIGH	AV:L/AC:M/Au:N/C:C/I:C/A:C	45.195.162.194	The shared memory manager (used by pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that bounds checks are enforced by all compilers, which might allow local users to gain privileges by leveraging access to a sandboxed privilege separation process, related to the m_zback and m_zlib data structures.
CVE-2015-5600	8.5	MEDIUM	AV:N/AC:M/Au:N/C:P/I:P/A:P	45.195.162.194	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption, resource leakage, and duplicate list in the sshd -oChallengeResponseAuthentication=yes option, as demonstrated by a modified client that provides a different password for each password prompt, aka SSHD-CVE-2015-5600.
CVE-2016-10009	7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	45.195.162.194	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.
CVE-2016-10708	5	MEDIUM	AV:N/AC:L/Au:N/C:N/I:N/A:P	45.195.162.194	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
CVE-2016-10011	4	MEDIUM	AV:N/AC:M/Au:N/C:P/I:P/A:N	45.195.162.194	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2016-10009	4.3	MEDIUM	AV:N/AC:M/Au:N/C:P/I:N/A:N	45.195.162.194	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-10010	4.3	MEDIUM	AV:N/AC:M/Au:N/C:P/I:N/A:N	45.195.162.194	The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows in-the-middle attackers to target cryptographically weaker connections if both peers support the strongest algorithm that is available to both of them.
CVE-2016-10011	6.5	MEDIUM	AV:N/AC:L/Au:S/C:P/I:P/A:N	45.195.162.194	Multiple CRLF injection vulnerabilities in sessions.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.

11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

www.linkedin.com › muhammad-talha-a0759660

Muhammad Talha - BMA Capital Management Limited

Manager, Money Market & Fixed Income at **BMA Capital** Management Limited. **BMA Capital** ...

Manager-FMR at Pak **Iran** Joint Investment Company. Pakistan.

Pakistan · Manager, Money Market & Fixed Income · BMA Capital Management Limited

The same Robtex search confirms the Iranian address is tied to the server in the Netherlands, which correlates to known OSINT of Iranian use of the Netherlands as a remote server (See Advanced Persistent Threats: APT33 and APT34):

12. A search of the indivisible.org network showed a subdomain which evidences the existence of scorecard software in use as part of the Indivisible (formerly ACORN) political group for Obama:

13. Each of the tabulation software companies have their own central reporting "affiliate". Edison Research is the affiliate for Dominion.
14. Beanfield.com out of Canada shows the connections via co-hosting related sites, including dvscorp.com:

This domain redirects to **beanfield.com**

DNS

View API →

A	96.45.195.194 5 Domains →
MX	10 barracuda.dominionvoting.com. 2 Domains →
NS	ns29.domaincontrol.com. 56,979,357 Domains →
	ns30.domaincontrol.com. 56,979,357 Domains →

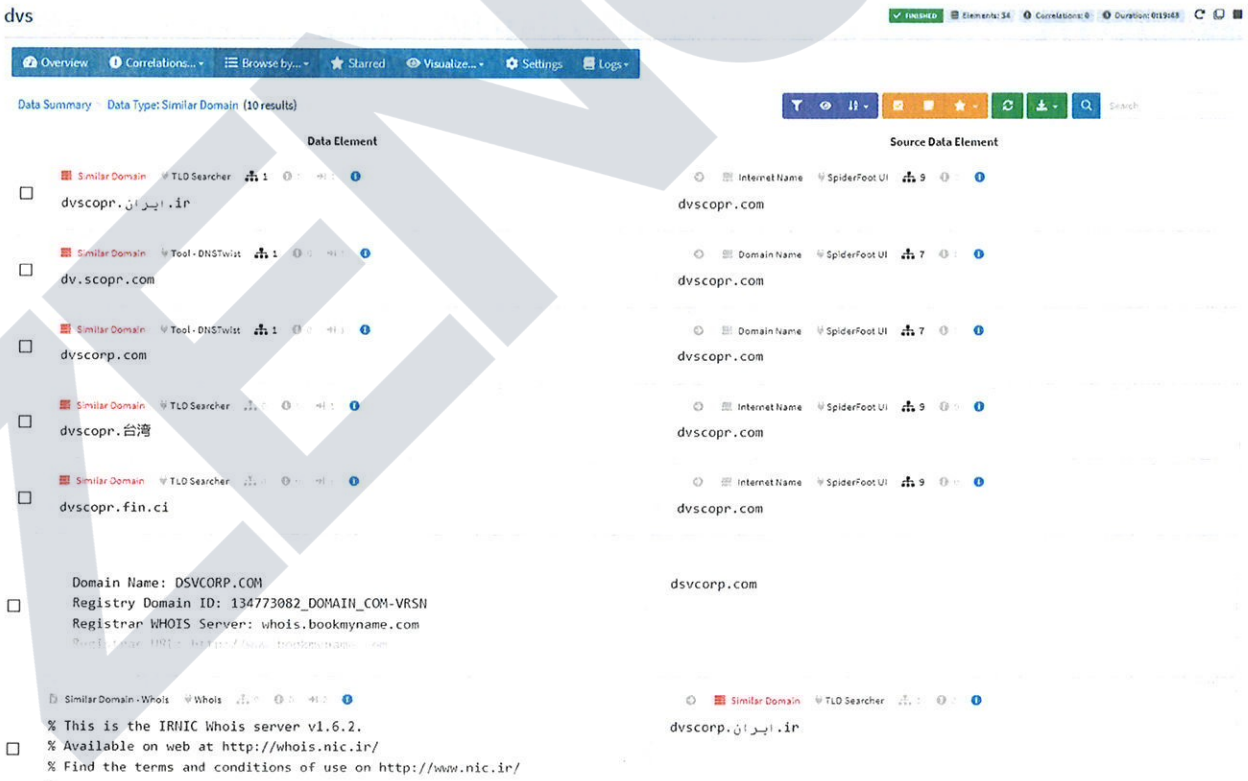
Co-Hosted

There are 5 domains hosted on 96.45.195.194 (AS21949 Beanfield Technologies Inc.) Show All →

View API →

guta.ca	ndbgroup.ca	dvscorp.com
aiyokuacardiolounge.com	grantdyer.com	

This Dominion partner domain “dvscorp” also includes an auto discovery feature, where new in-network devices automatically connect to the system. The following diagram shows some of the dvscorp.com mappings, which mimic the infrastructure for Dominion:



The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:

15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date recorded	Pages
050500/0236	Sep 25, 2019	Sep 26, 2019	7

Conveyance

SECURITY AGREEMENT

Assignors	Correspondent	Attorney docket
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020	

Assignee

HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

View all

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function--the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:

Patent assignment 050500/0236

SECURITY AGREEMENT

Date recorded	Reel/frame	Pages
Sep 26, 2019	050500/0236	7

Assignors
DOMINION VOTING SYSTEMS CORPORATION

Execution date
Sep 25, 2019

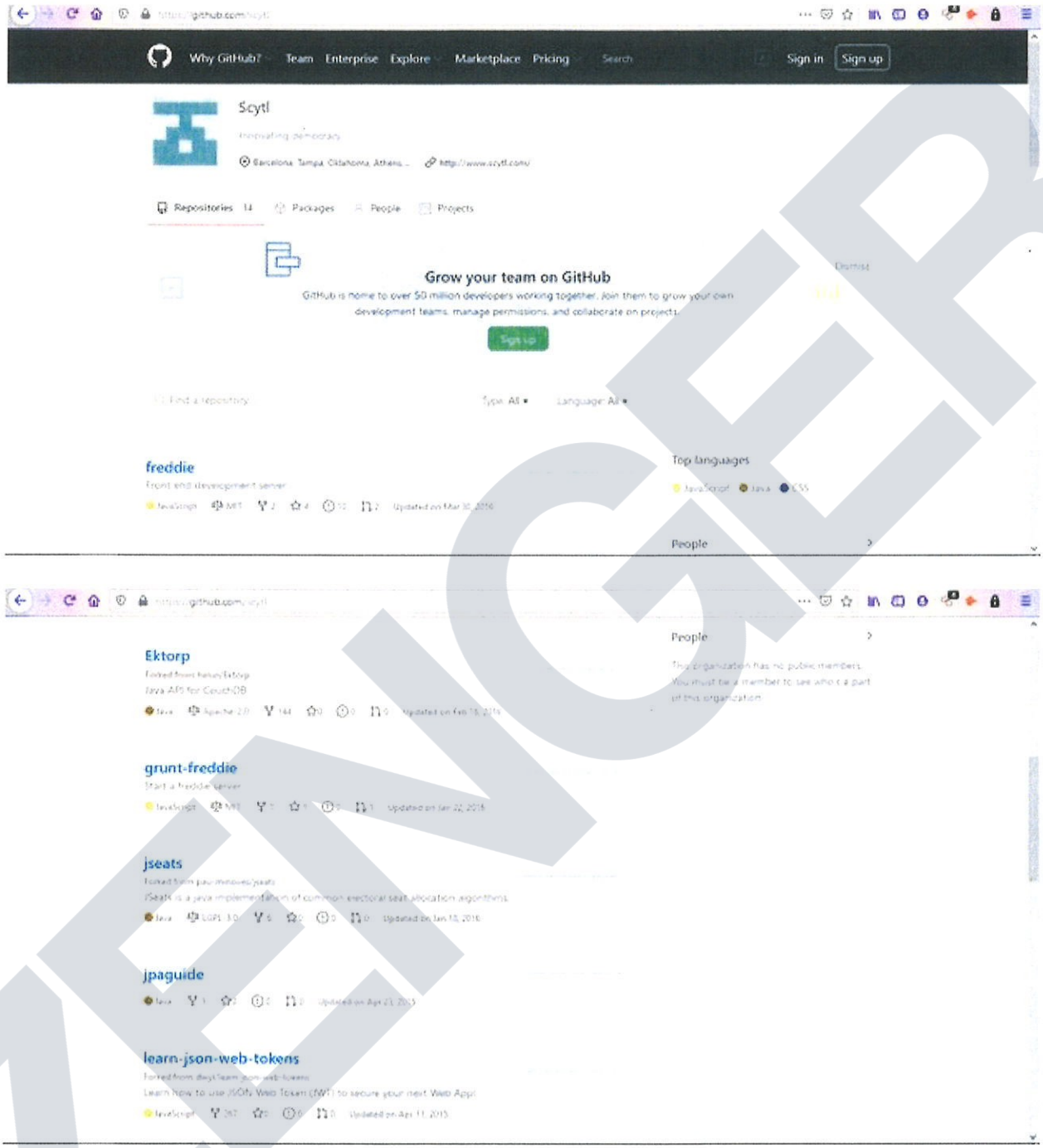
Assignee
HSBC BANK CANADA, AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET
TORONTO M5J 1S9
CANADA

Correspondent
CHAPMAN & CUTLER LLP
1270 AVENUE OF THE AMERICAS, 30TH FLOOR
ATTN: SOREN SCHWARTZ
NEW YORK, NY 10020

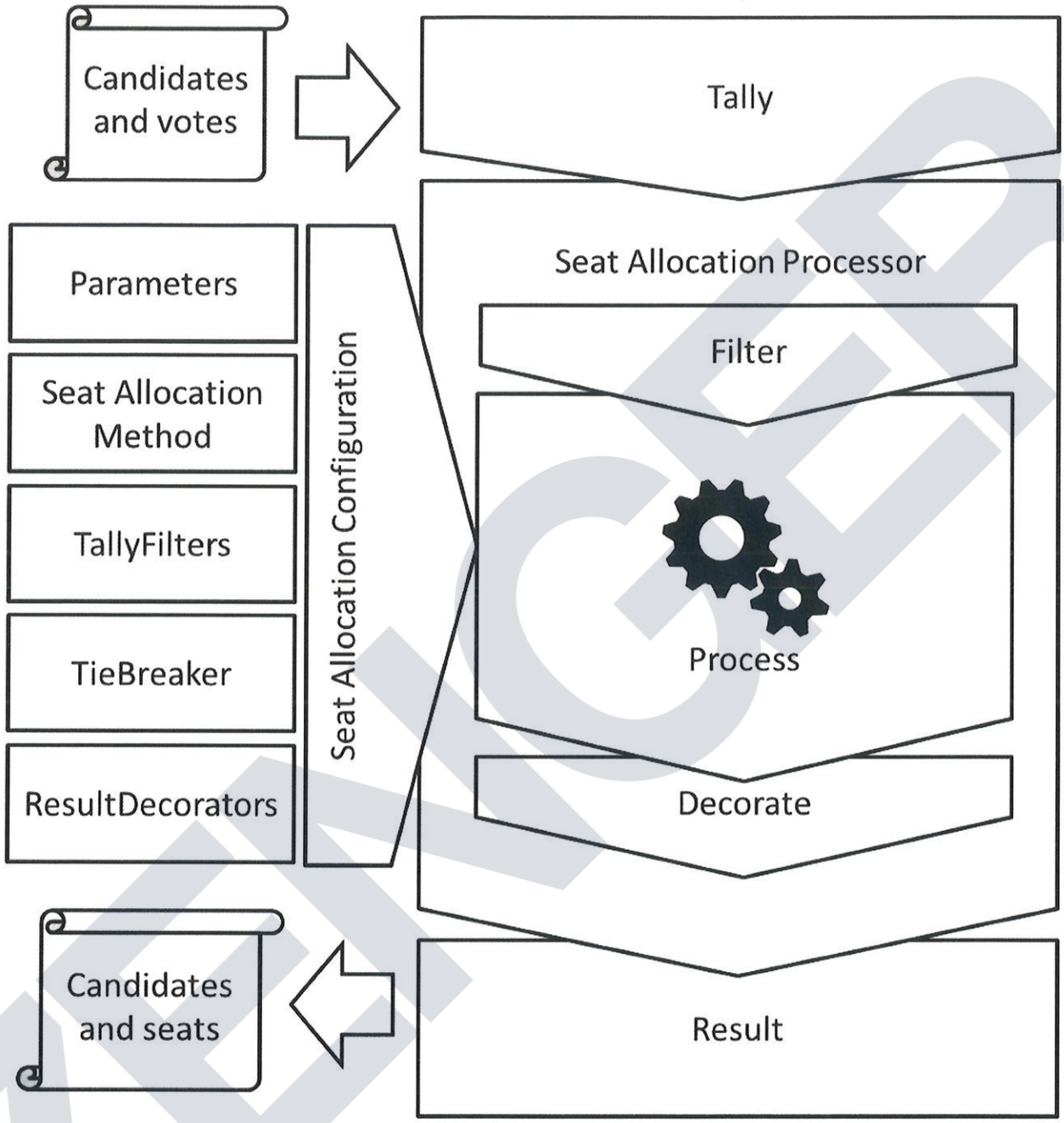
Properties (18 total)

Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN POULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC		
8195505 Jun 5, 2012	20050247783 Nov 10, 2005	11121997 May 5, 2005
3. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7422151 Sep 9, 2008	20070012767 Jan 18, 2007	11526028 Sep 25, 2006
4. BALLOT LEVEL SECURITY FEATURES FOR OPTICAL SCAN VOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION Inventors: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN		

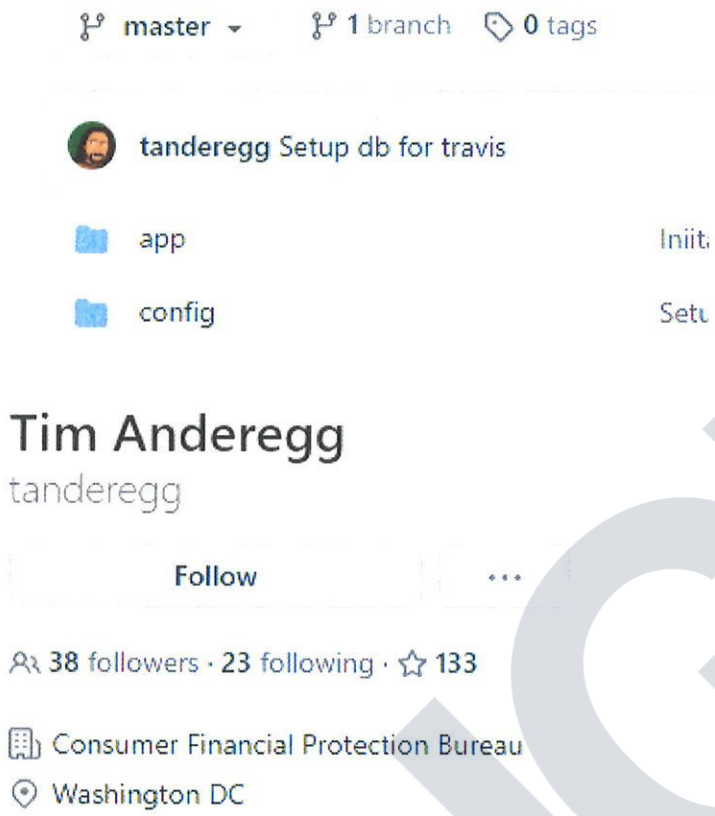
17. Smartmatic creates the backbone (like the cloud). CTCL is responsible for the security within the election system.



18. In the github account for Scytl, Scytl Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. A point of interest for the Center for Tech and Civic Life within their github page (https://github.com/ctcl) is that one of the programmers for Edison Research holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



20. As seen in included document titled "AA20-304A-Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data " that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.
21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgo knowledge. Executed this December 16th, 2020

Smartmatic SSL Certificate

Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted] make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. [redacted]
3. I am a US citizen and I reside at [redacted] in the United States of America.
4. Researching Smartmatic's website and reading their public manuals about the reuse of SSL certificate's, I started to investigate Smartmatic's SSL certificates. Upon searching their website is currently behind Cloudflare yet using the same SSL certificate it made it easy to locate where Smartmatic's website was located. Smartmatic's website is in the Philippine's on their Election commission's server (Comelec.gov.ph).

https://censys.io/domain?q=smartmatic.com

Censys

Websites smartmatic.com

Quick Filters

For all fields, see Data Definitions

Protocol:

1 25/smtp

Tag:

1 smtp

Websites

Page: 1/1 Results: 1 Time: 18ms

comelec.gov.ph (172.67.165.108)

117,344 25/smtp

https://censys.io/domain/comelec.gov.ph

Censys | Websites | comelec.gov.ph

comelec.gov.ph

Summary

Basic Information

Alexa Rank 117,344

Protocols 25/SMTP

Tags SMTP

443/HTTPS

DETAILS GO

25/SMTP

Banner Grab and StartTLS Initiation

DETAILS

Banner 220 sulat.comelec.gov.ph ESMTP ready.

EHLO 250-sulat.comelec.gov.ph Hello worker-04.sfj.censys-scanner.com [192.35.168.64]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-STARTTLS
250 HELP

STARTTLS 220 TLS go ahead

https://censys.io/domain/comelec.gov.ph

Censys | Websites | comelec.gov.ph

220 TLS go ahead

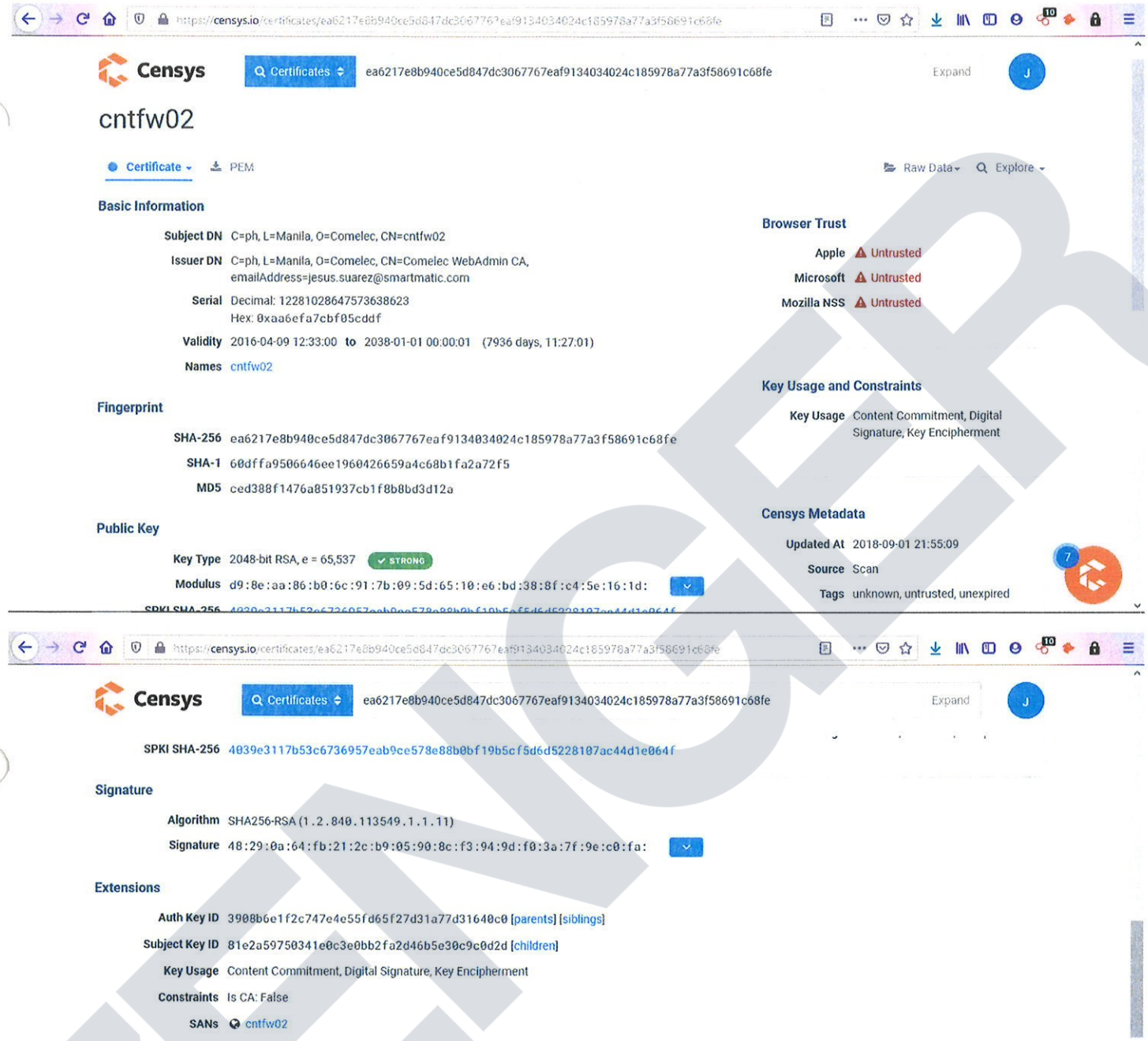
TLS Handshake

Version TLSv1.2

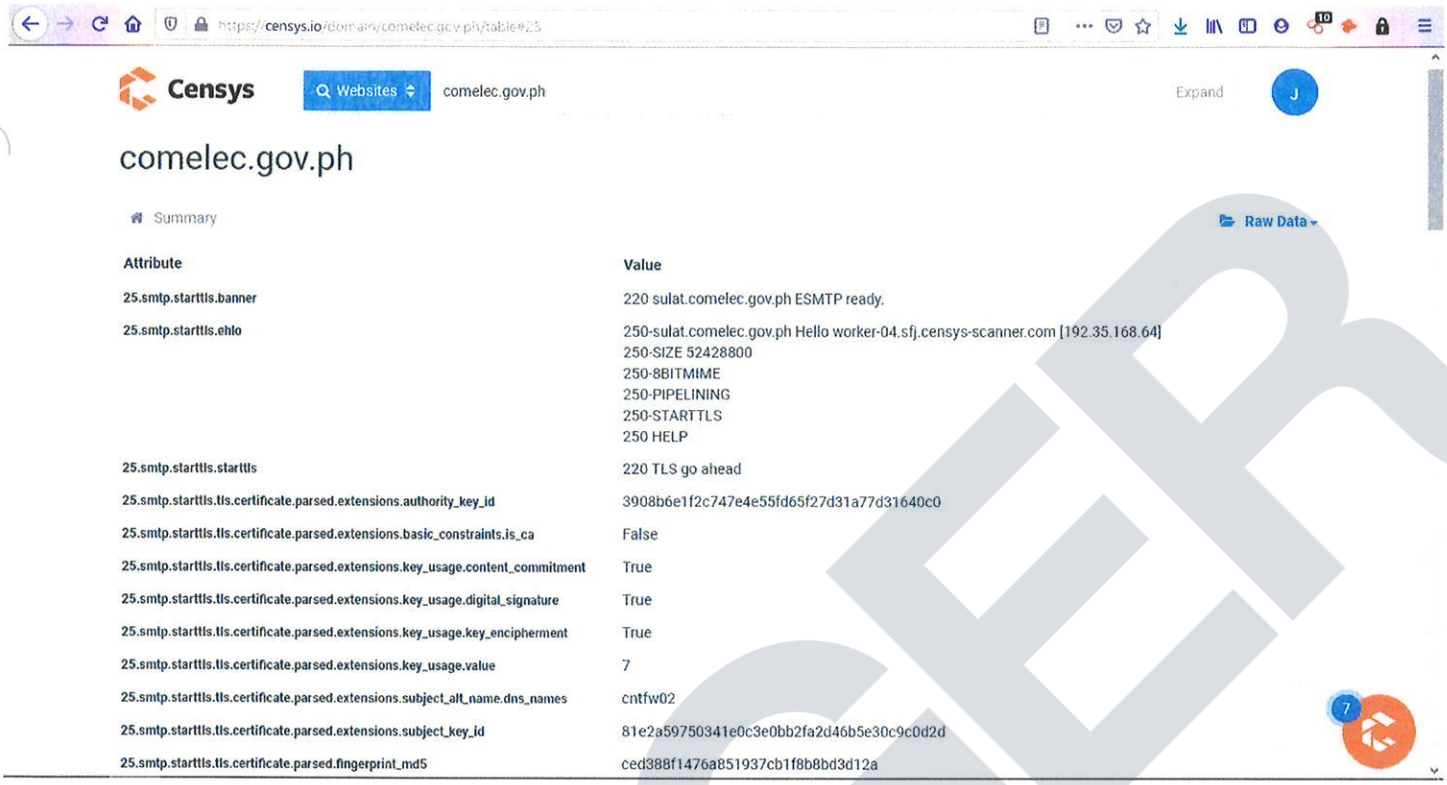
Cipher Suite TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)

Certificate Chain

ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
C=ph, L=Manila, O=Comelec, CN=cntfw02
C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com



5. As can be seen in the images above the SSL certificate used was registered by the email address jesus.suarez@smartmatic.com on the 9th of April 2016.

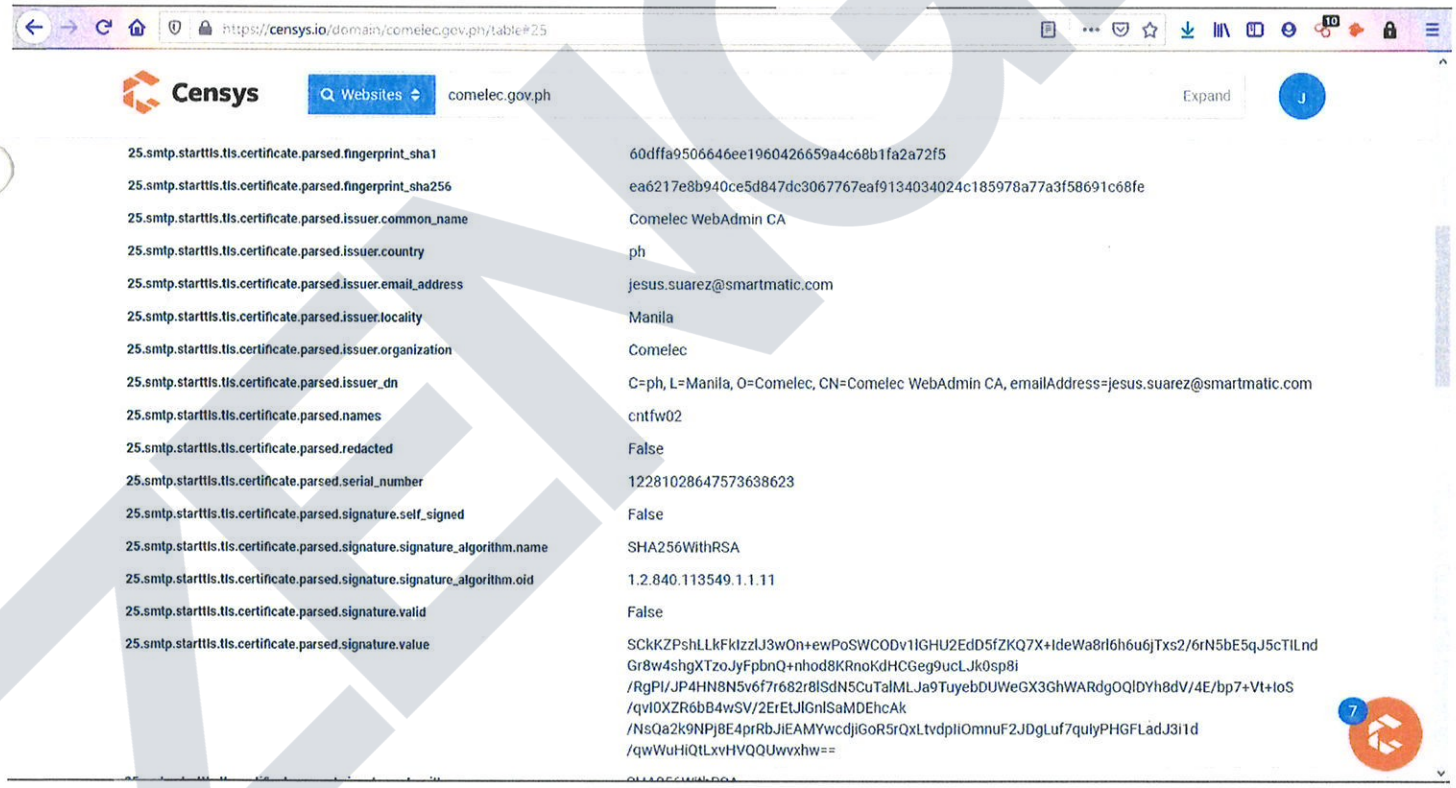


Censys | Websites | comelec.gov.ph | Expand | J

comelec.gov.ph

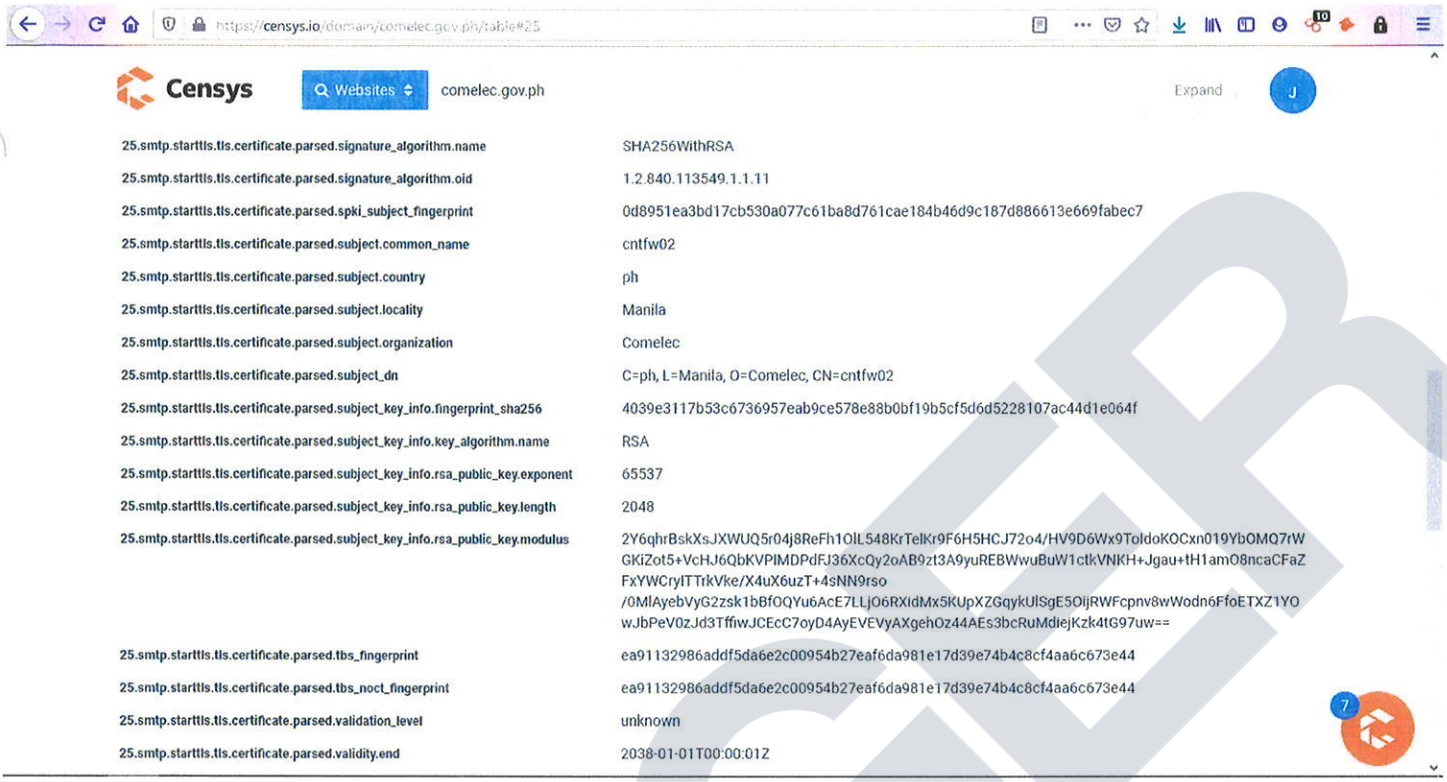
Summary | Raw Data

Attribute	Value
25.smtp.starttls.banner	220 sulat.comelec.gov.ph ESMTP ready.
25.smtp.starttls.ehlo	250-sulat.comelec.gov.ph Hello worker-04.sfj.censys-scanner.com [192.35.168.64] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
25.smtp.starttls.starttls	220 TLS go ahead
25.smtp.starttls.tls.certificate.parsed.extensions.authority_key_id	3908b6e1f2c747e4e55fd65f27d31a77d31640c0
25.smtp.starttls.tls.certificate.parsed.extensions.basic_constraints.is_ca	False
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.content_commitment	True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.digital_signature	True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.key_encipherment	True
25.smtp.starttls.tls.certificate.parsed.extensions.key_usage.value	7
25.smtp.starttls.tls.certificate.parsed.extensions.subject_alt_name.dns_names	cntfw02
25.smtp.starttls.tls.certificate.parsed.extensions.subject_key_id	81e2a59750341e0c3e0bb2fa2d46b5e30c9c0d2d
25.smtp.starttls.tls.certificate.parsed.fingerprint_md5	ced388f1476a851937cb1f8b8bd3d12a



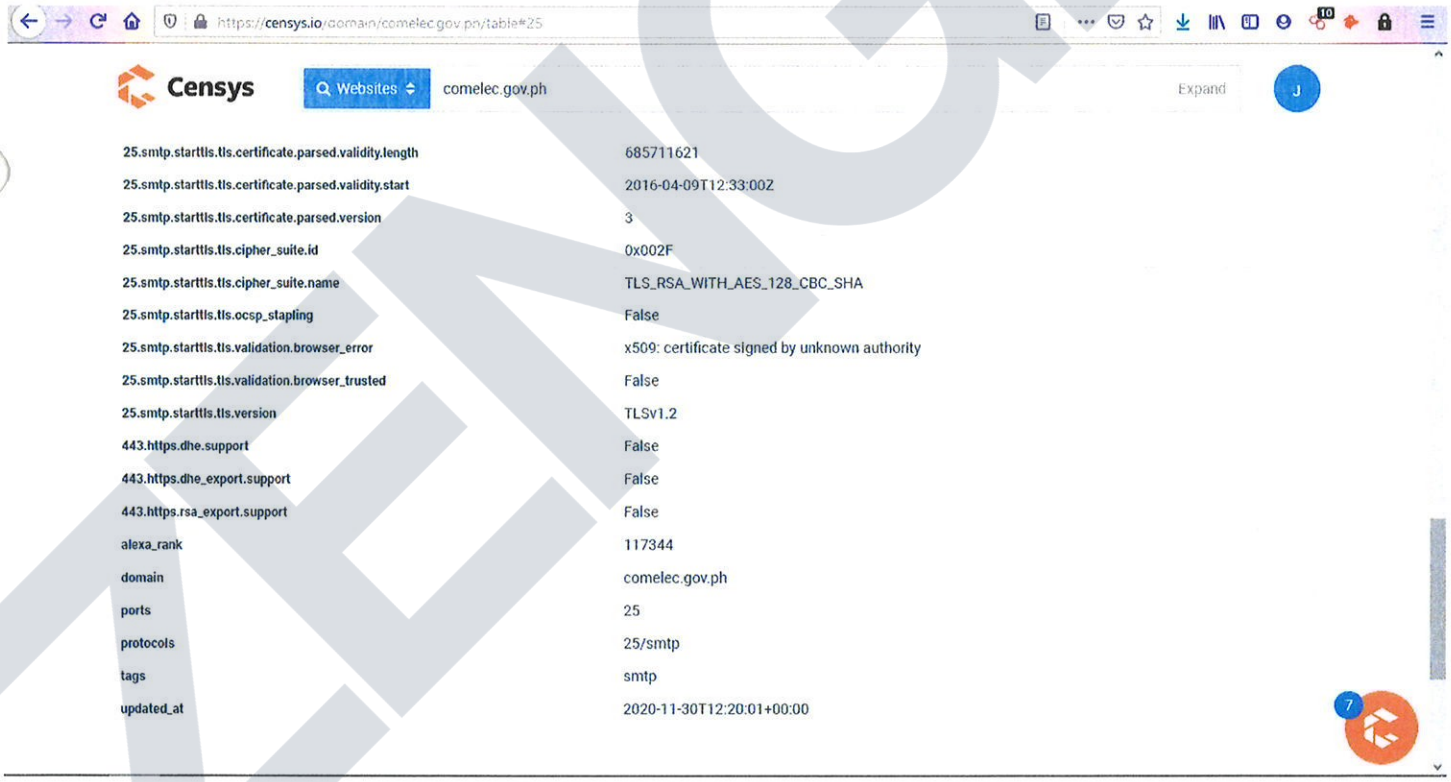
Censys | Websites | comelec.gov.ph | Expand | J

25.smtp.starttls.tls.certificate.parsed.fingerprint_sha1	60dffa9506646ee1960426659a4c68b1fa2a72f5
25.smtp.starttls.tls.certificate.parsed.fingerprint_sha256	ea6217e8b940ce5d847dc3067767eaf9134034024c185978a77a3f58691c68fe
25.smtp.starttls.tls.certificate.parsed.issuer.common_name	Comelec WebAdmin CA
25.smtp.starttls.tls.certificate.parsed.issuer.country	ph
25.smtp.starttls.tls.certificate.parsed.issuer.email_address	jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.issuer.locality	Manila
25.smtp.starttls.tls.certificate.parsed.issuer.organization	Comelec
25.smtp.starttls.tls.certificate.parsed.issuer_dn	C=ph, L=Manila, O=Comelec, CN=Comelec WebAdmin CA, emailAddress=jesus.suarez@smartmatic.com
25.smtp.starttls.tls.certificate.parsed.names	cntfw02
25.smtp.starttls.tls.certificate.parsed.redacted	False
25.smtp.starttls.tls.certificate.parsed.serial_number	12281028647573638623
25.smtp.starttls.tls.certificate.parsed.signature.self_signed	False
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.name	SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature.signature_algorithm.oid	1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.signature.valid	False
25.smtp.starttls.tls.certificate.parsed.signature.value	SCkKZPshLLkFkIzzlJ3wOn+ewPoSWCODv1lGHU2EdD5fZKQ7X+IdeWa8rl6h6u6jTxs2/6rN5bE5qJ5cTILnd Gr8w4shgXTzoJyFpbnQ+nhod8KRnoKdHCGeg9ucLJk0sp8i /RgPl/JP4HN8N5v6f7r682r8lSdN5CuTalMLJa9TuyebDUWeGX3GhWARdgOQlDYh8dV/4E/bp7+Vt+IoS /qvI0XZR6bB4wSV/2ErEtJlGnlSaMDEhcAk /NsQa2k9NPj8E4prRbJiEAMYwcdjiGoR5rQxLtvdpIiOmnuF2JDgLuf7qulyPHGFLadJ3i1d /qwWuHiQtLxvHVQQUwvxhw==



Censys | Websites | comelec.gov.ph | Expand | J

25.smtp.starttls.tls.certificate.parsed.signature_algorithm.name	SHA256WithRSA
25.smtp.starttls.tls.certificate.parsed.signature_algorithm.oid	1.2.840.113549.1.1.11
25.smtp.starttls.tls.certificate.parsed.spki_subject_fingerprint	0d8951ea3bd17cb530a077c61ba8d761cae184b46d9c187d886613e669fabec7
25.smtp.starttls.tls.certificate.parsed.subject.common_name	cntfw02
25.smtp.starttls.tls.certificate.parsed.subject.country	ph
25.smtp.starttls.tls.certificate.parsed.subject.locality	Manila
25.smtp.starttls.tls.certificate.parsed.subject.organization	Comelec
25.smtp.starttls.tls.certificate.parsed.subject_dn	C=ph, L=Manila, O=Comelec, CN=cntfw02
25.smtp.starttls.tls.certificate.parsed.subject_key_info.fingerprint_sha256	4039e3117b53c6736957eab9ce578e88b0bf19b5cf5d6d5228107ac44d1e064f
25.smtp.starttls.tls.certificate.parsed.subject_key_info.key_algorithm.name	RSA
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.exponent	65537
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.length	2048
25.smtp.starttls.tls.certificate.parsed.subject_key_info.rsa_public_key.modulus	2Y6qhrBskXsJXWUQ5r04j8ReFh1OlL548KrTelKr9F6H5HCJ72o4/HV9D6Wx9ToldoKOCxn019YbOMQ7rW GKiZot5+VcHJ6QbKVPIMDPdFJ36XcQy2oAB9zt3A9yuREBWwuBuW1ctkVNKH+Jgau+tH1amO8ncaCFaZ FxYWCryITTrkVke/X4uX6uzT+4sNN9rso /0MlAyebVyG2zsk1bBfOQYu6AcE7LLjO6RXidMx5KUpXZGqykUlSgE5OijRWFcpnv8wWodn6FfoETXZ1YO wJbPeV0zJd3TffiwJCEcC7oyD4AyEVEVyAXgehOz44AEs3bcRuMdiejKzk4tG97uw==
25.smtp.starttls.tls.certificate.parsed.tbs_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.tbs_noct_fingerprint	ea91132986addf5da6e2c00954b27eaf6da981e17d39e74b4c8cf4aa6c673e44
25.smtp.starttls.tls.certificate.parsed.validation_level	unknown
25.smtp.starttls.tls.certificate.parsed.validity.end	2038-01-01T00:00:01Z

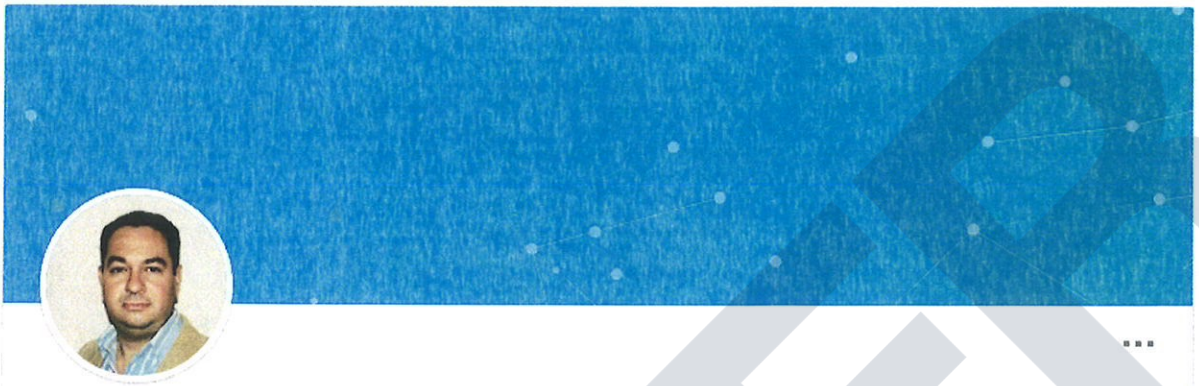


Censys | Websites | comelec.gov.ph | Expand | J

25.smtp.starttls.tls.certificate.parsed.validity.length	685711621
25.smtp.starttls.tls.certificate.parsed.validity.start	2016-04-09T12:33:00Z
25.smtp.starttls.tls.certificate.parsed.version	3
25.smtp.starttls.tls.cipher_suite.id	0x002F
25.smtp.starttls.tls.cipher_suite.name	TLS_RSA_WITH_AES_128_CBC_SHA
25.smtp.starttls.tls.ocsp_stapling	False
25.smtp.starttls.tls.validation.browser_error	x509: certificate signed by unknown authority
25.smtp.starttls.tls.validation.browser_trusted	False
25.smtp.starttls.tls.version	TLSv1.2
443.https.dhe.support	False
443.https.dhe_export.support	False
443.https.rsa_export.support	False
alexa_rank	117344
domain	comelec.gov.ph
ports	25
protocols	25/smtp
tags	smtp
updated_at	2020-11-30T12:20:01+00:00

https://es.linkedin.com/in/jesusalbertosuarez

LinkedIn People Jesús Alberto Suárez Méndez



Jesús Alberto Suárez Méndez

Senior Consultant at VISEO IBERIA

Alcorcón, Community of Madrid, Spain · 500+ connections

Join to Connect

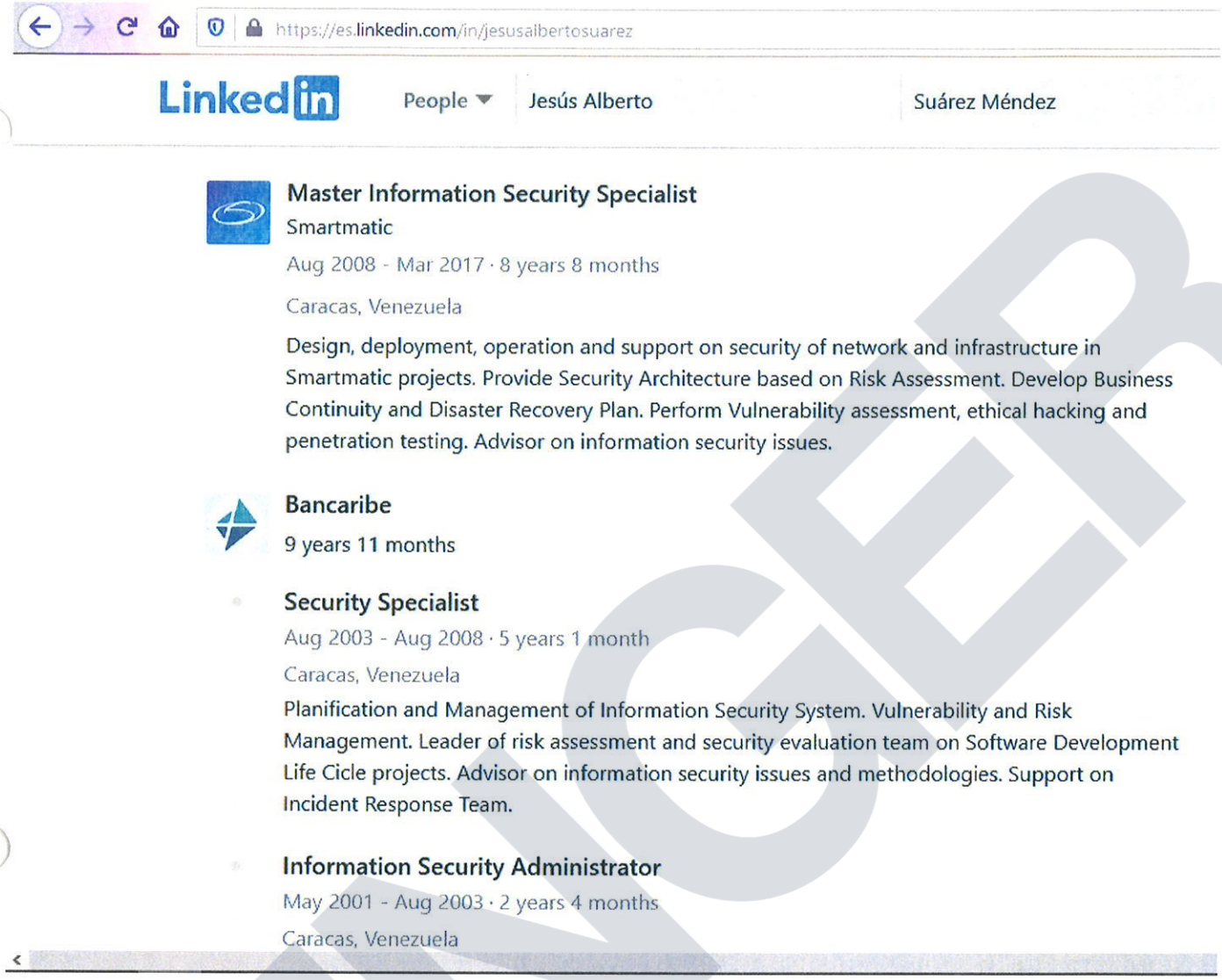
VISEO IBERIA

Universidad de los Andes (VE)

Blog

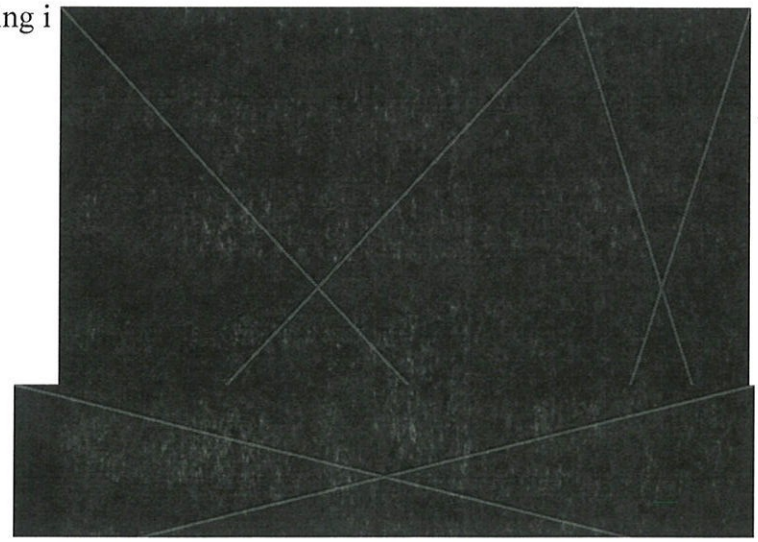
About

DevOps SysAdmin and Information Security Professional with more than 20 years of experience. Specialized in Security and IT Management, IT Risk Assessment and Management, IT architecture, automatized deployments on Linux environment and cloud using DevOps tools. Very interested in



6. As seen from Jesus' LinkedIn profile, he was employed by Smartmatic as their Master Information Security Specialist from August 2008 – March 2017, within the time frame of the registered SSL certificate for Smartmatic and within Venezuela.
7. This evidence shows that Smartmatic was indeed connected to Venezuela as well as shows that their dealings with the Philippine's is still on-going as their website is in their election commission servers with matching and current SSL certificates.

I declare under penalty of perjury that the forgoing i d this December 16th, 2020.



DECLARATION OF [redacted]

I, [redacted], hereby state the following:

1. [redacted]

2. I am an adult of sound mine. All statements in this declaration are based on my personal knowledge and are true and correct.

3. I am making this statement voluntarily and on my own initiative. I have not been promised, nor do I expect to receive, anything in exchange for my testimony and giving this statement. I have no expectation of any profit or reward and understand that there are those who may seek to harm me for what I say in this statement. I have not participated in any political process in the United States, have not supported any candidate for office in the United States, am not legally permitted to vote in the United States, and have never attempted to vote in the United States.

4. I want to alert the public and let the world know the truth about the corruption, manipulation, and lies being committed by a conspiracy of people and companies intent upon betraying the honest people of the United States and their legally constituted institutions and fundamental rights as citizens. This conspiracy began more than a decade ago in Venezuela and has spread to countries all over the world. It is a conspiracy to wrongfully gain and keep power and wealth. It involves political leaders, powerful companies, and other persons whose purpose is to gain and keep power by changing the free will of the people and subverting the proper course of governing.

5. [redacted] Over the course of my career, I specialized in the marines [redacted]

6. Due to my training in special operations and my extensive military and academic formations, I was selected for the national security guard detail of the President of Venezuela. [redacted]

[redacted]

7. [redacted] Señor Cabello was a long-time confederate of President Chavez and instrumental in his gaining power. In 2002, Señor Cabello had very briefly taken over the duties of the presidency while Hugo Chavez was imprisoned. Within hours of Señor Cabello taking over the presidency, Hugo Chavez was released from prison and regained the office of President. On December 11, 2011, Cabello was installed as the Vice-President of the United Socialist Party – the party of President Chávez and became the second most powerful figure in the party after Hugo Chávez. Cabello was appointed president of the National Assembly in early 2012 and was re-elected to that post in January 2013. After Hugo Chávez's death, Cabello was next in line for the presidency of the country, but he remained president of the National Assembly and yielded to Nicolás Maduro holding the position of President of Venezuela.

8. [redacted] President Chavez was very precise and exacting in his instructions in the details about meetings he wanted, where the meeting was to occur, who was to attend, what was to be done. [redacted]

9. [redacted] I was witness to the creation and operation of a

sophisticated electronic voting system that permitted the leaders of the Venezuelan government to manipulate the tabulation of votes for national and local elections and select the winner of those elections in order to gain and maintain their power.

10. Importantly, I was a direct witness to the creation and operation of an electronic voting system in a conspiracy between a company known as Smartmatic and the leaders of conspiracy with the Venezuelan government. This conspiracy specifically involved President Hugo Chavez Frias, the person in charge of the National Electoral Council named Jorge Rodriguez, and principals, representatives, and personnel from Smartmatic which included [redacted]. The purpose of this conspiracy was to create and operate a voting system that could change the votes in elections from votes *against* persons running the Venezuelan government to votes *in their favor* in order to maintain control of the government.

11. In mid-February of 2009, there was a national referendum to change the Constitution of Venezuela to end term limits for elected officials, including the President of Venezuela. The referendum passed. This permitted Hugo Chavez to be re-elected an unlimited number of times.

12. After passage of the referendum, President Chavez instructed me to make arrangements for him to meet with Jorge Rodriguez, then President of the National Electoral Council, and three executives from Smartmatic. Among the three Smartmatic representatives were [redacted] President Chavez had multiple meetings with Rodriguez and the Smartmatic team at which I was present. In the first of four meetings, Jorge Rodriguez promoted the idea to create software that would manipulate elections. Chavez was very excited and made it clear that he would provide whatever Smartmatic needed. He wanted them immediately to create a voting system which would ensure that any time anything was going to be voted on the voting system would guarantee results that Chavez wanted. Chavez offered Smartmatic many inducements, including large sums of money, for Smartmatic to create or modify the voting system so that it would guarantee Chavez would win every election cycle. Smartmatic's team agreed to create such a system and did so.

13. I arranged and attended three more meetings between President Chavez and the representatives from Smartmatic at which details of the new

voting system were discussed and agreed upon. For each of these meetings, I communicated directly with [redacted] on details of where and when to meet, where the participants would be picked up and delivered to the meetings, and what was to be accomplished. At these meetings, the participants called their project the "Chavez revolution." From that point on, Chavez never lost any election. In fact, he was able to ensure wins for himself, his party, Congress persons and mayors from townships.

14. Smartmatic's electoral technology was called "Sistema de Gestión Electoral" (the "Electoral Management System"). Smartmatic was a pioneer in this area of computing systems. Their system provided for transmission of voting data over the internet to a computerized central tabulating center. The voting machines themselves had a digital display, fingerprint recognition feature to identify the voter, and printed out the voter's ballot. The voter's thumbprint was linked to a computerized record of that voter's identity. Smartmatic created and operated the entire system.

15. Chavez was most insistent that Smartmatic design the system in a way that the system could change the vote of each voter without being detected. He wanted the software itself to function in such a manner that if the voter were to place their thumb print or fingerprint on a scanner, then the thumbprint would be tied to a record of the voter's name and identity as having voted, but that voter would not tracked to the changed vote. He made it clear that the system would have to be setup to not leave any evidence of the changed vote for a specific voter and that there would be no evidence to show and nothing to contradict that the name or the fingerprint or thumb print was going with a changed vote. Smartmatic agreed to create such a system and produced the software and hardware that accomplished that result for President Chavez.

16. After the Smartmatic Electoral Management System was put in place, I closely observed several elections where the results were manipulated using Smartmatic software. One such election was in December 2006 when Chavez was running against Rosales. Chavez won with a landslide over Manuel Rosales - a margin of nearly 6 million votes for Chavez versus 3.7 million for Rosales.

17. On April 14, 2013, I witnessed another Venezuelan national election in which the Smartmatic Electoral Management System was used to manipulate and change the results for the person to succeed Hugo Chávez

as President. In that election, Nicolás Maduro ran against Capriles Radonsky. [redacted] Inside that location was a control room in which there were multiple digital display screens – TV screens – for results of voting in each state in Venezuela. The actual voting results were fed into that room and onto the displays over an internet feed, which was connected to a sophisticated computer system created by Smartmatic. People in that room were able to see in "real time" whether the vote that came through the electronic voting system was in their favor or against them. If one looked at any particular screen, they could determine that the vote from any specific area or as a national total was going against either candidate. Persons controlling the vote tabulation computer had the ability to change the reporting of votes by moving votes from one candidate to another by using the Smartmatic software.

18. By two o'clock in the afternoon on that election day Capriles Radonsky was ahead of Nicolás Maduro by two million votes. When Maduro and his supporters realized the size of Radonsky's lead they were worried that they were in a crisis mode and would lose the election. The Smartmatic machines used for voting in each state were connected to the internet and reported their information over the internet to the Caracas control center in real-time. So, the decision was made to reset the entire system. Maduro's and his supporters ordered the network controllers to take the internet itself offline in practically all parts in Venezuela and to change the results.

19. It took the voting system operators approximately two hours to make the adjustments in the vote from Radonsky to Maduro. Then, when they turned the internet back on and the on-line reporting was up and running again, they checked each screen state by state to be certain where they could see that each vote was changed in favor of Nicholas Maduro. At that moment the Smartmatic system changed votes that were for Capriles Radonsky to Maduro. By the time the system operators finish, they had achieved a convincing, but narrow victory of 200,000 votes for Maduro.

20. After Smartmatic created the voting system President Chavez wanted, he exported the software and system all over Latin America. It was sent to Bolivia, Nicaragua, Argentina, Ecuador, and Chile – countries that were in alliance with President Chavez. This was a group of leaders who wanted to be able to guarantee they maintained power in their countries. When Chavez died, Smartmatic was in a position of being the only

company that could guarantee results in Venezuelan elections for the party in power.

21. I want to point out that the software and fundamental design of the electronic electoral system and software of Dominion and other election tabulating companies relies upon software that is a descendant of the Smartmatic Electoral Management System. In short, the Smartmatic software is in the DNA of every vote tabulating company's software and system.

22. Dominion is one of three major companies that tabulates votes in the United States. Dominion uses the same methods and fundamentally same software design for the storage, transfer and computation of voter identification data and voting data. Dominion and Smartmatic did business together. The software, hardware and system have the same fundamental flaws which allow multiple opportunities to corrupt the data and mask the process in a way that the average person cannot detect any fraud or manipulation. The fact that the voting machine displays a voting result that the voter intends and then prints out a paper ballot which reflects that change does not matter. It is the software that counts the digitized vote and reports the results. The software itself is the one that changes the information electronically to the result that the operator of the software and vote counting system intends to produce that counts. That's how it is done. So the software, the software itself configures the vote and voting result -- changing the selection made by the voter. The software decides the result regardless of what the voter votes.

23. All of the computer controlled voting tabulation is done in a closed environment so that the voter and any observer cannot detect what is taking place unless there is a malfunction or other event which causes the observer to question the process. I saw first-hand that the manipulation and changing of votes can be done in real-time at the secret counting center which existed in Caracas, Venezuela. For me it was something very surprising and disturbing. I was in awe because I had never been present to actually see it occur and I saw it happen. So, I learned first-hand that it doesn't matter what the voter decides or what the paper ballot says. It's the software operator and the software that decides what counts – not the voter.

24. If one questions the reliability of my observations, they only have to read the words of [redacted] a time period in

which Smartmatic had possession of all the votes and the voting, the votes themselves and the voting information at their disposition in Venezuela. [redacted] he was assuring that the voting system implemented or used by Smartmatic was completely secure, that it could not be compromised, was not able to be altered.

25. But later, in 2017 when there were elections where Maduro was running and elections for legislators in Venezuela, [redacted] and Smartmatic broke their secrecy pact with the government of Venezuela. He made a public announcement through the media in which he stated that all the Smartmatic voting machines used during those elections were totally manipulated and they were manipulated by the electoral council of Venezuela back then. [redacted] stated that all of the votes for Nicholas Maduro and the other persons running for the legislature were manipulated and they actually had lost. So I think that's the greatest proof that the fraud can be carried out and will be denied by the software company that [redacted] admitted publicly that Smartmatic had created, used and still uses vote counting software that can be manipulated or altered.

26. I am alarmed because of what is occurring in plain sight during this 2020 election for President of the United States. The circumstances and events are eerily reminiscent of what happened with Smartmatic software electronically changing votes in the 2013 presidential election in Venezuela. What happened in the United States was that the vote counting was abruptly stopped in five states using Dominion software. At the time that vote counting was stopped, Donald Trump was significantly ahead in the votes. Then during the wee hours of the morning, when there was no voting occurring and the vote count reporting was off-line, something significantly changed. When the vote reporting resumed the very next morning there was a very pronounced change in voting in favor of the opposing candidate, Joe Biden.

27. [redacted] I have worked in gathering information, researching, and working with information technology. That's what I know how to do and the special knowledge that I have. Due to these recent election events, I contacted a number of reliable and intelligent ex-co-workers of mine that are still informants and work with the intelligence community. I asked for them to give me information that was up-to-date information in as far as how all these businesses are acting, what actions they are taking.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was prepared in Dallas County, State of Texas, and executed on November 15, 2020.

[redacted]

Executive Orders

Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

Issued on: September 12, 2018

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that the ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States. Although there has been no evidence of a foreign power altering the outcome or vote tabulation in any United States election, foreign powers have historically sought to exploit America's free and open political system. In recent years, the proliferation of digital devices and internet-based communications has created significant vulnerabilities and magnified the scope and intensity of the threat of foreign interference, as illustrated in the 2017 Intelligence Community Assessment. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. 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.

(b) Within 45 days of receiving the assessment and information described in section 1(a) of this order, the Attorney General and the Secretary of Homeland Security, in consultation with the heads of any other appropriate agencies and, as appropriate, State and local officials, shall deliver to the President, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense a report evaluating, with respect to the United States election that is the subject of the assessment described in section 1(a):

(i) the extent to which any foreign interference that targeted election infrastructure materially affected the security or integrity of that infrastructure, the tabulation of votes, or the timely transmission of election results; and

(ii) if any foreign interference involved activities targeting the infrastructure of, or pertaining to, a political organization, campaign, or candidate, the extent to which such activities materially affected the security or integrity of that infrastructure, including by unauthorized access to, disclosure or threatened disclosure of, or alteration or falsification of, information or data.

The report shall identify any material issues of fact with respect to these matters that the Attorney General and the Secretary of Homeland Security are unable to evaluate or reach agreement on at the time the report is submitted. The report shall also include updates and recommendations, when appropriate, regarding remedial actions to be taken by the United States Government, other than the sanctions described in sections 2 and 3 of this order.

(c) Heads of all relevant agencies shall transmit to the Director of National Intelligence any information relevant to the execution of the Director's duties pursuant to this order, as appropriate and consistent with applicable law. If relevant information emerges after the submission of the report mandated by section 1(a) of this order, the Director, in consultation with the heads of any other appropriate agencies, shall amend the report, as appropriate, and the Attorney General and the Secretary of Homeland Security shall amend the report required by section 1(b), as appropriate.

(d) Nothing in this order shall prevent the head of any agency or any other appropriate official from tendering to the President, at any time through an appropriate channel, any analysis, information, assessment, or evaluation of foreign interference in a United States election.

(e) If information indicating that foreign interference in a State, tribal, or local election within the United States has occurred is identified, it may be included, as appropriate, in the assessment mandated by section 1(a) of this order or in the report mandated by section 1(b) of this order, or submitted to the President in an independent report.

(f) Not later than 30 days following the date of this order, the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall develop a framework for the process that will be used to carry out their respective responsibilities pursuant to this order. The framework, which may be classified in whole or in part, shall focus on ensuring that agencies fulfill their responsibilities pursuant to this order in a manner that maintains methodological consistency; protects law enforcement or other sensitive information and intelligence sources and methods; maintains an appropriate

separation between intelligence functions and policy and legal judgments; ensures that efforts to protect electoral processes and institutions are insulated from political bias; and respects the principles of free speech and open debate.

Sec. 2. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any foreign person determined by the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security:

(i) to have directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election;

(ii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsection (a)(i) of this section or any person whose property and interests in property are blocked pursuant to this order; or

(iii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to this order.

(b) Executive Order 13694 of April 1, 2015, as amended by Executive Order 13757 of December 28, 2016, remains in effect. This order is not intended to, and does not, serve to limit the Secretary of the Treasury's discretion to exercise the authorities provided in Executive Order 13694. Where appropriate, the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, may exercise the authorities described in Executive Order 13694 or other authorities in conjunction with the Secretary of the Treasury's exercise of authorities provided in this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

Sec. 3. Following the transmission of the assessment mandated by section 1(a) and the report mandated by section 1(b):

(a) the Secretary of the Treasury shall review the assessment mandated by section 1(a) and the report mandated by section 1(b), and, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security, impose all appropriate sanctions pursuant to section 2(a) of this order and any appropriate sanctions described in section 2(b) of this order; and

(b) the Secretary of State and the Secretary of the Treasury, in consultation with the heads of other appropriate agencies, shall jointly prepare a recommendation for the President as to whether additional sanctions against foreign persons may be appropriate in response to the identified foreign interference and in light of the evaluation in the report mandated by section 1(b) of this order, including, as appropriate and consistent with applicable law, proposed sanctions with respect to the largest business entities licensed or domiciled in a country whose government authorized, directed, sponsored, or supported election interference, including at least one entity from each of the following sectors: financial services, defense, energy, technology, and transportation (or, if inapplicable to that country's largest business entities, sectors of comparable strategic significance to that foreign government). The recommendation shall include an assessment of the effect of the recommended sanctions on the economic and national security interests of the United States and its allies. Any recommended sanctions shall be appropriately calibrated to the scope of the foreign interference identified, and may include one or more of the following with respect to each targeted foreign person:

(i) blocking and prohibiting all transactions in a person's property and interests in property subject to United States jurisdiction;

(ii) export license restrictions under any statute or regulation that requires the prior review and approval of the United States Government as a condition for the export or re-export of goods or services;

(iii) prohibitions on United States financial institutions making loans or providing credit to a person;

(iv) restrictions on transactions in foreign exchange in which a person has any interest;

(v) prohibitions on transfers of credit or payments between financial institutions, or by, through, or to any financial institution, for the benefit of a person;

(vi) prohibitions on United States persons investing in or purchasing equity or debt of a person;

(vii) exclusion of a person's alien corporate officers from the United States;

(viii) imposition on a person's alien principal executive officers of any of the sanctions described in this section; or

(ix) any other measures authorized by law.

Sec. 4. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order would seriously impair my ability to deal with the national emergency declared in this order, and I hereby prohibit such donations as provided by section 2 of this order.

Sec. 5. The prohibitions in section 2 of this order include the following:

(a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and

(b) the receipt of any contribution or provision of funds, goods, or services from any such person.

Sec. 6. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens whose property and interests in property are blocked pursuant to this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 7. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 8. For the purposes of this order:

(a) the term "person" means an individual or entity;

(b) the term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(c) the term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person (including a foreign person) in the United States;

(d) the term "election infrastructure" means information and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results;

(e) the term "United States election" means any election for Federal office held on, or after, the date of this order;

(f) the term "foreign interference," with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions;

(g) the term "foreign government" means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States;

(h) the term "covert," with respect to an action or attempted action, means characterized by an intent or apparent intent that the role of a foreign government will not be apparent or acknowledged publicly; and

(i) the term "State" means the several States or any of the territories, dependencies, or possessions of the United States.

Sec. 9. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 2 of this order.

Sec. 10. Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof.

Sec. 11. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may re-delegate any of these functions to other officers within the Department of the Treasury consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

Sec. 12. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 13. This order shall be implemented consistent with 50 U.S.C. 1702(b)(1) and (3).

Sec. 14. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,

September 12, 2018.

WhiteHouse.gov

50 U.S. Code § 1702 - Presidential authorities

(a) In general

(1) At the times and to the extent specified in section 1701 of this title, the President may, under such regulations as he may prescribe, by means of instructions, licenses, or otherwise— (A) investigate, regulate, or prohibit—

(i)

any transactions in foreign exchange,

(ii)

transfers of credit or payments between, by, through, or to any banking institution, to the extent that such transfers or payments involve any interest of any foreign country or a national thereof,

(iii)

the importing or exporting of currency or securities,

by any person, or with respect to any property, subject to the jurisdiction of the United States;

(B)

investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States; and.[1]

(C) when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States; and all right, title, and interest in any property so confiscated shall vest, when, as, and upon the terms directed by the President, in such agency or person as the President may designate from time to time, and upon such terms and conditions as the President may prescribe, such interest or property shall be held, used, administered, liquidated, sold, or otherwise dealt with in the interest of and for the benefit of the United States, and such designated agency or person may perform any and all acts incident to the accomplishment or furtherance of these purposes.

(2)

In exercising the authorities granted by paragraph (1), the President may require any person to keep a full record of, and to furnish under oath, in the form of reports or otherwise, complete information relative to any act or transaction referred to in paragraph (1) either before, during, or after the completion thereof, or relative to any interest in foreign property, or relative to any property in which any foreign country or any national thereof has or has had any interest, or as may be otherwise necessary to enforce the provisions of such paragraph. In any case in which a report by a person could be required under this paragraph, the President may require the production of any books of account, records, contracts, letters, memoranda, or other papers, in the custody or control of such person.

(3)

Compliance with any regulation, instruction, or direction issued under this chapter shall to the extent thereof be a full acquittance and discharge for all purposes of the obligation of the person making the same. No person shall be held liable in any court for or with respect to anything done or omitted in good faith in connection with the administration of, or pursuant to and in reliance on, this chapter, or any regulation, instruction, or direction issued under this chapter.
(b) Exceptions to grant of authorityThe authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly—
(1)
any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value;
(2)
donations, by persons subject to the jurisdiction of the United States, of articles, such as food, clothing, and medicine, intended to be used to relieve human suffering, except to the extent that the President determines that such donations (A) would seriously impair his ability to deal with any national emergency declared under section 1701 of this title, (B) are in response to coercion against the proposed recipient or donor, or (C) would endanger Armed Forces of the United States which are engaged in hostilities or are in a situation where imminent involvement in hostilities is clearly indicated by the circumstances; or [2]
(3)
the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 4604 [3] of this title, or under section 4605 [3] of this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of title 18; or
(4)
any transactions ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use, maintenance within any country including payment of living expenses and acquisition of goods or services for personal use, and arrangement or facilitation of such travel including nonscheduled air, sea, or land voyages. (c) Classified information

In any judicial review of a determination made under this section, if the determination was based on classified information (as defined in section 1(a) of the Classified Information Procedures Act) such information may be submitted to the reviewing court ex parte and in camera. This subsection does not confer or imply any right to judicial review.

(Pub. L. 95–223, title II, § 203, Dec. 28, 1977, 91 Stat. 1626; Pub. L. 100–418, title II, § 2502(b)(1), Aug. 23, 1988, 102 Stat. 1371; Pub. L. 103–236, title V, § 525(c)(1), Apr. 30, 1994, 108 Stat. 474; Pub. L. 107–56, title I, § 106, Oct. 26, 2001, 115 Stat. 277.)

Congress of the United States

Washington, DC 20515

October 6, 2006

Henry M. Paulson, Jr.
Secretary
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

Dear Mr. Secretary:

I am writing to follow up on my letter of May 4, 2006, to Secretary Snow, seeking review by the Committee on Foreign Investment in the United States of the acquisition of Sequoia Voting Systems by Smartmatic, a foreign-owned company. I believe this transaction raises exactly the sort of foreign ownership issues that CFIUS is best positioned to examine for national security concerns. As discussed below, publicly reported information about Smartmatic's ownership and about the vulnerability of electronic voting machines to tampering raises serious concerns. I strongly urge CFIUS to independently verify the information provided to American officials and the public by Sequoia/Smartmatic, and to take all appropriate measures to safeguard our national security.

It is undisputed that Smartmatic is foreign-owned and it has acquired Sequoia, one of the three major voting machine companies doing business in the U.S. According to a Sequoia press release in May 2006 (copy attached) Sequoia voting machines were used to record over 125 million votes during the 2004 Presidential election in the United States. As we confront another election, Americans deserve to know that the Administration has made sure that any foreign ownership of voting machines poses no national security threat.

Although many press reports have tried, it appears that it is not possible to discern the true owners of Smartmatic from information available to the public. Smartmatic now acknowledges that Antonio Mugica, a Venezuelan businessman, has a controlling interest in Smartmatic, but the company has not revealed who all the other Smartmatic owners are. According to the press, Smartmatic's owners are hidden through a web of off-shore private entities. (See attached articles.)

The opaque nature of Smartmatic's ownership is particularly troubling since Smartmatic has been associated by the press with the Venezuelan government led by Hugo Chavez, which is openly hostile to the United States. According to press reports, Smartmatic shared a founder, officers, directors and a principal place of business with Bizta, a company in which, according to Smartmatic, the Venezuelan government previously held a 28% stake. Mugica is also a director of Bizta.

According to Smartmatic press releases, (copies attached) Smartmatic and Bizta were part of the consortium that received the government contract to provide the voting machines for the 2004 referendum election to recall Chavez as Venezuela's president, and have since been awarded other contracts by the Venezuelan government.

Smartmatic's possible connection to the Venezuelan government poses a potential national security concern in the context of its acquisition of Sequoia because electronic voting machines are susceptible to tampering and insiders are in the best position to engage in such tampering. The 2005 Government Accountability Office Report on electronic voting, GAO-05-956, and other private sector studies consistently support this conclusion. Thus, the reports that Sequoia brought Venezuelan nationals to the United States to work on the Chicago 2006 primary election raises questions about whether these individuals are subject to direction from a foreign interest that might pose a threat to the integrity of the election. Similarly, the use of Smartmatic software and machines developed in Venezuela, such as the HAAT software that was at issue in Chicago, raises questions as to whether this software is susceptible to manipulation by its unknown creators. Reportedly, Smartmatic may soon be introducing into the United States the type of electronic voting machines that were used (with Bizta software) in the controversial 2004 Venezuelan recall election, under the label AVC Edge II Plus.

In reviewing the Smartmatic acquisition of Sequoia, it is important that CFIUS understand the products and services that are of Venezuelan origin and evaluate Smartmatic's ownership to determine who could have influence and control over these and other Sequoia products and services that are in use or intended for use in U.S. elections. In light of Smartmatic's failure fully to answer these questions to date, this issue demands the most thorough independent investigation by CFIUS.

Thank you for your consideration of this letter.

Sincerely,

Carolyn B. Maloney

Carolyn B. Maloney
Member of Congress

Attachments

Congress of the United States

Washington, DC 20510

December 6, 2019

Michael McCarthy
Chairman
McCarthy Group, LLC
[redacted]

Dear Mr. McCarthy:

We are writing to request information regarding McCarthy Group, LLC's (McCarthy Group) investment in Election Systems & Software (ES&S), one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.[1] For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"[2] owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."[3] In light of these concerns, we request that you provide information about your firm, the portfolio companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early

---

[1] Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

[2] ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

[3] Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

2000s, almost twenty vendors competed in the election technology market.[4] Today, three large vendors—ES&S, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.[5] Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance."[6] While experts estimate that the total revenue for election technology vendors is about $300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.[7]

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems–leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[8] In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span … [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."[9]

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election officials in addressing these risks.[10] However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our

---

[4] Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

[5] Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[6] Id.

[7] Id.

[8] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[9] U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

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

elections at avoidable and increased risk.[11] In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured."[12] Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers."[13]

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana."[14] In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states."[15] And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem."[16] These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

McCarthy Group reportedly owns or has had investments in ES&S, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.[17]

2. Which election technology companies, including all affiliates or related entities, does McCarthy Group have a stake in or own? Please provide the name of and a brief description of the services each company provides.

    a. Which election technology companies, including all affiliates or related entities, has McCarthy Group had a stake in or owned in the past twenty

---

[11] AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[12] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

[13] Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019, https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

[14] Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

[15] Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

[16] New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.

[17] Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

years? Please provide the name of and a brief description of the services each company provides or provided.

b. For each election technology company McCarthy Group had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
   i. The name of the company
   ii. Ownership stake
   iii. Total revenue
   iv. Net income
   v. Percentage of revenue dedicated to research and development
   vi. Total number of employees
   vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
   viii. Other private-equity firms that own a stake in the company

3. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.

4. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.

5. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.

6. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the

past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren
United States Senator

Amy Klobuchar
United States Senator

Ron Wyden
United States Senator

Mark Pocan
Member of Congress

Congress of the United States

Washington, DC 20510

December 6, 2019

Sami Mnaymneh
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC
[redacted]

Tony Tamer
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC
[redacted]

Dear Messrs. Mnaymneh and Tamer:

We are writing to request information regarding H.I.G. Capital's (H.I.G.) investment in Hart InterCivic Inc. (Hart InterCivic) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.[1] For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"[2] owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."[3] In light of these concerns, we request that you provide information about your firm, the portfolio

---

[1] Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

[2] ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

[3] Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.[4] Today, three large vendors—Election Systems & Software, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.[5] Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance."[6] While experts estimate that the total revenue for election technology vendors is about $300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.[7]

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems–leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[8] In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span … [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."[9]

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election

---

[4] Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

[5] Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[6] Id.

[7] Id.

[8] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[9] U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

officials in addressing these risks.[10] However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.[11] In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured."[12] Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers."[13]

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana."[14] In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states."[15] And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem."[16] These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

H.I.G. reportedly owns or has had investments in Hart InterCivic, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.[17]

2. Which election technology companies, including all affiliates or related entities, does H.I.G. have a stake in or own? Please provide the name of and a brief description of the services each company provides.

---

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

[11] AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[12] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

[13] Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019, https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1.

[14] Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

[15] Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

[16] New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.

[17] Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

a. Which election technology companies, including all affiliates or related entities, has H.I.G. had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.

b. For each election technology company H.I.G. had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
   i. The name of the company
   ii. Ownership stake
   iii. Total revenue
   iv. Net income
   v. Percentage of revenue dedicated to research and development
   vi. Total number of employees
   vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
   viii. Other private-equity firms that own a stake in the company

3. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.

4. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.

5. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.

6. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren
United States Senator

Amy Klobuchar
United States Senator

Ron Wyden
United States Senator

Mark Pocan
Member of Congress

Congress of the United States

Washington, DC 20510

December 6, 2019

Stephen D. Owens
Managing Director
Staple Street Capital Group, LLC
[redacted]

Hootan Yaghoobzadeh
Managing Director
Staple Street Capital Group, LLC
[redacted]

Dear Messrs. Owens and Yaghoobzadeh:

We are writing to request information regarding Staple Street Capital Group, LLC's (Staple Street) investment in Dominion Voting System (Dominion) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.[1] For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"[2] owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."[3] In light of these concerns, we request that you provide information about your firm, the portfolio

---

[1] Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html.

[2] ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

[3] Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.[4] Today, three large vendors—Election Systems & Software, Dominion, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.[5] Private equity firms reportedly own or control each of these vendors, with very limited "information available in the public domain about their operations and financial performance."[6] While experts estimate that the total revenue for election technology vendors is about $300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.[7]

Concentration in the election technology market and the fact that vendors are often "more seasoned in voting machine and technical services contract negotiations" than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems–leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[8] In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider "the cost to purchase or lease, operate, and maintain a voting system over its life span … [and to] know how the vendor(s) plan to be profitable" when signing contracts, because vendors typically make their profits by ensuring "that they will be around to maintain it after the sale." The EAC has warned election officials that "[i]f you do not manage the vendors, they will manage you."[9]

Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States' election infrastructure as "critical infrastructure" in order to prioritize the protection of our elections and to more effectively assist state and local election

---

[4] Bloomberg, "Private Equity Controls the Gatekeepers of American Democracy," Anders Melin and Reade Pickert, November 3, 2018, https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

[5] Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[6] Id.

[7] Id.

[8] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

[9] U.S. Election Assistance Commission, "Ten Things to Know About Selecting a Voting System," October 14, 2017, https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/.

officials in addressing these risks.[10] However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.[11] In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state "using some machines that are no longer manufactured."[12] Moreover, even when state and local officials work on replacing antiquated machines, many continue to "run on old software that will soon be outdated and more vulnerable to hackers."[13]

In 2018 alone "voters in South Carolina [were] reporting machines that switched their votes after they'd inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana."[14] In addition, researchers recently uncovered previously undisclosed vulnerabilities in "nearly three dozen backend election systems in 10 states."[15] And, just this year, after the Democratic candidate's electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county's Republican Chairwoman said, "[n]othing went right on Election Day. Everything went wrong. That's a problem."[16] These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

Staple Street reportedly owns or has had investments in Dominion, a major election technology vendor. In order to help us understand your firm's role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.[17]

2. Which election technology companies, including all affiliates or related entities, does Staple Street have a stake in or own? Please provide the name of and a brief description of the services each company provides.

---

[10] Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.
[11] AP News, "US election integrity depends on security-challenged firms," Frank Bajak, October 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c; Penn Wharton Public Policy Initiative, "The Business of Voting," July 2018, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.
[12] Brennan Center for Justice, "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.
[13] Associated Press, "AP Exclusive: New election systems use vulnerable software," Tami Abdollah, July 13, 2019, https://apnews.com/e5c070c31f3c497fa9e6875f426ccde1.
[14] Vice, "Here's Why All the Voting Machines Are Broken and the Lines Are Extremely Long," Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.
[15] Vice, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.
[16] New York Times, "A Pennsylvania Country's Election Day Nightmare Underscores Voting Machine Concerns," Nick Corasaniti, November 30, 2019, https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html.
[17] Stop Wall Street Looting Act, S.2155, https://www.congress.gov/bill/116th-congress/senate-bill/2155.

a. Which election technology companies, including all affiliates or related entities, has Staple Street had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.

b. For each election technology company Staple Street had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
   i. The name of the company
   ii. Ownership stake
   iii. Total revenue
   iv. Net income
   v. Percentage of revenue dedicated to research and development
   vi. Total number of employees
   vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
   viii. Other private-equity firms that own a stake in the company

3. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.

4. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.

5. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.

6. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren
United States Senator

Amy Klobuchar
United States Senator

Ron Wyden
United States Senator

Mark Pocan
Member of Congress

COMMUNITIES DIGITAL NEWS

Commentary ◇ Featured ◇ Patriot Profiles by Jeanne McKinney ◇ Politics

Swiss and Aussies find a critical flaw in Scytl software that the US ignores

written by Jeanne McKinney | Nov 18, 2020

SAN DIEGO: How is it the Swiss and Aussies were better positioned to handle voting than the U.S.? They vetted Scytl online voting software and discovered alarming features. Due diligence proved Scytl software not secure, not verifiable end to end. They must have known a bad electronic voting system could put the wrong candidate in office. They cared enough to prevent that from happening in their countries.

SwissPost intended to roll out an online voting system to "boost participation" and "deliver faster results than postal counts. Australia thought it could be more convenient, too. So, they contacted respected academics to dive into the software code.

Vanessa Teague, (professor at the University of Melbourne at the time) is known for her work on secret sharing, cryptographic protocols, and the security of electronic voting. Teague teamed up to evaluate Scytl with an international group of researchers.

They published a report on March 12, 2019, called "The use of trapdoor commitments in Bayer-Groth proofs and he implications for the verifiability of the Scytl-SwissPost Internet voting system*"

The researchers probed the "shuffling and decryption components of Switzerland's online voting system." Their 'act relevant to New South Wales' iVote online system because both were developed by Scytl, a company headquartered in Barcelona [and Frankfurt] that specializes in secure electronic voting," says InnovationAus .

Attorney Sidney Powell: Protecting America from hacked voting software

Aussies, Swiss found back door to future election disaster.

Online or mail-in voting may seem like a solution to a world trying to survive a raging COVID-19 pandemic. But without thorough vetting – it's like giving criminal minds a gun AND the ammunition. When you send an electronic vote it's floating through nebulous, unquantified cyberspace. It may solve getting to the polls in a physical sense and getting votes counted quickly. But it doesn't change the challenges of control of information.

> **On Mar 12, 2019, MIT published a technology review on the Scytl research, "A cryptographic trap door could let someone change votes cast using Switzerland's online sVote system without being detected, according to a new paper."**
>
> Vice News reported same day,
> **"The cryptographic backdoor exists in a part of the system that is supposed to verify that all of the ballots and votes counted in an election are the same ones that voters cast. But the flaw could allow someone to swap out all of the legitimate ballots and replace them with fraudulent ones, all without detection," says Vice.**
>
> **"The vulnerability is astonishing," said Matthew Green, who teaches cryptography at Johns Hopkins University and did not do the research but read the researchers' report. "In normal elections, there is no single person who could undetectably defraud the entire election. But in this system they built, there is a party who could do that," adds Vice.**

11,354 Votes

Did Democrats steal the election?

Yes

No

I'm not sure

John Hopkins, MIT, two highly-ranked U.S. universities, warned of severe problems with Scytl-Swiss software system. Are academic opinions of naught? Which leads to why not? It appears that massive numbers of U.S. votes sailed in a leaky Scytl cyber craft from the U.S. across the seas to Germany and came back CHANGED.

Lawyer Sidney Powell: Democrats used Dominion machines to steal votes

What did the SwissPost/Aussie researchers find?

As best understood by this writer, the researchers said they couldn't state one way or the other if Scytl was less than expert at what they do or if they purposely created exploitable flaws. They are clear that the software is flawed and can be hacked. They state that it would be a good cover to write immature code which attempts to follow a published encryption method and that their flawed implementation could more easily be forgiven for doing so.

Or was the revealed flaw a feature for nefarious use?

The academic research asserts that Scytl followed the Bayer – Groth encryption method. Although they general followed the algorithm, they say Scytl failed to protect key pieces of data. They also said the data can be hacked, changing votes without a trace.

You would need to be expert in the algorithm to understand the specific critiques in the paper.

Election stealing issue in Scytl-SwissPost Internet voting system.

> **"Verifiability is a critical part of the trustworthiness of e-voting systems. Universal verifiability means that a proof of proper election conduct should be verifiable by any member of the public," says the report.**
>
> **"This mixnet has a trapdoor – a malicious administrator or software provider for the mix could manipulate votes but produce a proof transcript that passes verification. Thus complete verifiability fails," concludes the researchers.**

Sarah Jamie Lewis (former computer scientist for British Government Communications Headquarters (GCHQ) intelligence agency) was a critical member of the team. She says, ***"No election system should have a backdoor that allows the people running the election the ability to undetectably modify the election outcome…***

> *"We have only examined a tiny fraction of this code base and found a critical, election-stealing issue," says Lewis.*

Where was U.S. security, oversight for the 2020 Election?

"SwissPost, Switzerland's national postal service, published its shuffling and decryption code six months before it intended to use it for an election so that researchers like Professor Teague and colleague Lewis could vet the system for flaws," says InnovationAus. Olivier Pereira was also on the research team.

findings led researchers to recommend the Swiss government immediately halt plans to implement the system more widely. But it was bigger than Switzerland. Scytl provides electronic voting services to 35 countries, (including the U.S.)

Scytl said it was working on the Swiss [evote] flaw. That it managed to creep into the system in the first place worried MIT reviewers. The outcome is unknown. Scytl's statement on Swiss online major flaw.

We now know Scytl software cycled millions of U.S. votes. Lawyers work relentlessly to find out how many were modified in the 2020 election.

George Orwell's dystopian 1984 arrives in 2020: RIP America

Hackers could kick back and say 'who do you want to win'?

Russ Ramsland, Co-owner Allied Security Operations Group, was interviewed days leading up to the election. Excerpts about his findings:

> *"There are no [U.S.] national security standards that a voting company needs to meet. The software is so bad, you can easily change the audit trail, so later you cannot forensically go back and find out the votes that were changed," says Ramsland.*
>
> *"What happens to your vote after whatever the local voting company does to it? It turns out in the case of Texas and 27 other states – it goes to a [Scytl] server in Frankfurt Germany, owned by Barcelona Spain Multinational and that's actually who controls and reports your vote," he clarified.*

So your vote in Texas or anywhere in 28 states (including battleground) connects you to some foreign power. Were voters informed of this chicanery or allowed consent to this? Of course not, the perpetrators thought it would remain hidden.

Ramsland said they could see malware collecting credentials of county workers who submit voting information up, allowing a bad actor to go back into the county and change votes not just in Frankfurt, but the U.S. too.

The 2020 election failed to inform or protect voters.

Our understanding of reality is changed each day by Trump's lawyers and legal helpers, headed up by tireless Sidney Powell. They will certainly prove in court Scytl software a very bad risk, like the Swiss and Aussies. They will dig deep to find those bad actors. Hats off to all who took the hard steps to report election fraud. Keep stepping.

If voters knew on November 3rd what we now know, there would have been no election.

Americans' trust in electronic voting systems has been blown to smithereens. This scheme to wipe out Trump's legitimate votes is massive, complex, and unAmerican. Truth, the most powerful force, lies with the president and his allies searching for the monsters defiling the 2020 election. Yet alas, "The Kraken," is here to fight.

Breaking news: Huge win for Trump in Michigan.

Featured Image:
Composite Artwork Dave McKinney
United States in North America Map TUBS https://commons.wikimedia.org/wiki/File:United_States_in_North_America_(-mini_map_-rivers).svg
Flag Map of Germany David Liuzzo and AxG https://commons.wikimedia.org/wiki/File:Flag_map_of_Germany.svg
Curved Arrow Amada44 https://commons.wikimedia.org/wiki/File:Curved_Arrow.svg
Germany in Europe TUBS https://commons.wikimedia.org/wiki/File:Germany_in_Europe.svg
I Voted Sticker Dwight Burdette https://commons.wikimedia.org/wiki/File:I_Voted_Sticker.JPG
Math Formulas Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf

SPONSORED CONTENT ON CDN

From The Web

According To CGI, This Is What Historical Figures Really Looked Like

Taco Relish

The Israeli-made face mask Everyone Is Talking About in the US

The Jerusalem Post

Maps That Show Us A New Perspective

Explored Planet

AUSSIE | SCYTL | SOFTWARE FLAW | SWISS | VOTING

JEANNE MCKINNEY

Jeanne McKinney is an award-winning writer whose focus and passion is our United States active-duty military members and military news. Her Patriot Profiles offer an inside look at the amazing active-duty men and women in all Armed Services, including U.S. Marine Corps, Navy, Army, Air Force, Coast Guard, and National Guard. Reporting includes first-hand accounts of combat missions in Iraq and Afghanistan, the fight against violent terror groups, global defense, tactical training and readiness, humanitarian and disaster relief assistance, next-generation defense technology, family survival at home, U.S. port and border protection and illegal interdiction, women in combat, honoring the Fallen, Wounded Warriors, Military Working Dogs, Crisis Response, and much more. McKinney has won twelve San Diego Press Club "Excellence in Journalism Awards", including seven First Place honors.

previous post
George Orwell's dystopian 1984 arrives in 2020: RIP America

next post
Lt. Gen McInerney enters the voter fray: Dems used Intelligence software

Sponsored

Arabs and Russians find a critical flaw in Boyd software that the US ignores

Sponsored

SEARCH

Type and hit enter...

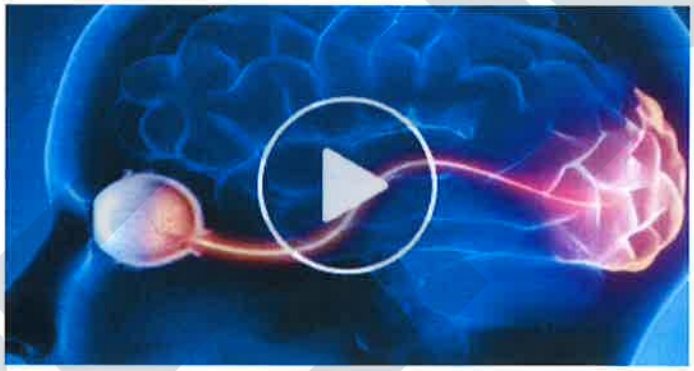
KEEP IN TOUCH

- ☐ FACEBOOK
- ☐ TWITTER
- ☐ INSTAGRAM
- ☐ PINTEREST
- ☐ LINKEDIN

Which president did more to protect our 2nd Amendment rights? (Free Gift For All Who Answer)

Obama Trump

1,842 Votes



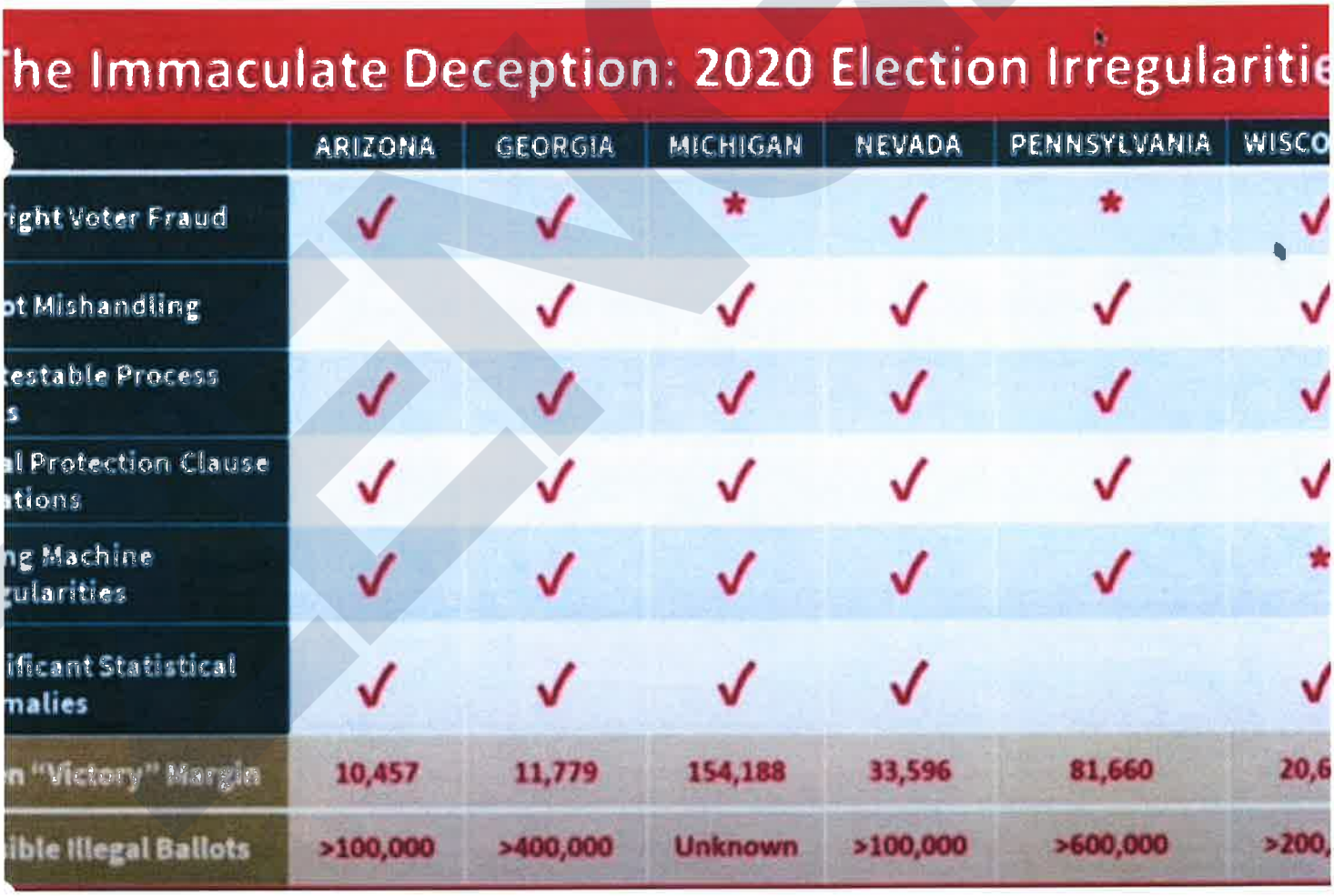
Big Pharma Doesn't Want You To Know About This Eyesight Trick

36,067

Who do you trust more?

President Trump | Doctor Fauci

RECENT POSTS



The Coup of America: Navarro says election was theft by a thousand cuts

1960's Nixon vs. Kennedy guide Congress on overturning election fraud

Knowing software would swap votes, did Dems choose Dominion?

Canelo vs Smith: Feliz Navidad for boxing fans Saturday

Big Drama Show hits blackjack: Golovkin sets record with 21st title defense Friday

AL GOODWYN CARTOONS

Al Goodwyn Cartoon: All is calm, no left anarchist too bright

Al Goodwyn Cartoon: The Democrat Parties new face?

Is it time for Joe Biden and Kamala Harris to consider conceding?

Veterans Day 2020: A time to honor our vets, present and past

Americans need Congress to pass "The New Voting Rights Act"

POPULAR POSTS

1

The 2015 Tour de France – Race Slideshow

President George Washington warns against political divisiveness

2

Jack is Back: Halloween Horror Nights at Universal Orlando

USEFUL LINKS

Contact

Privacy Policy

Cookie Policy

Media / Advertising

Who We Are / Masthead

Write for CommDigiNews

CommDigiNews Writer Directory

STORY CALENDAR

December 2020

M	T	W	T	F	S	S
	1	**2**	**3**	**4**	5	**6**
7	**8**	**9**	**10**	**11**	**12**	**13**
14	**15**	**16**	**17**	**18**	**19**	20
21	22	23	24	25	26	27
28	29	30	31			

« Nov

THE IMMACULATE DECEPTION:

Six Key Dimensions of Election Irregularities

The Navarro Report

Executive Summary

This report assesses the fairness and integrity of the 2020 Presidential Election by examining six dimensions of alleged election irregularities across six key battleground states. Evidence used to conduct this assessment includes more than 50 lawsuits and judicial rulings, thousands of affidavits and declarations,[1] testimony in a variety of state venues, published analyses by think tanks and legal centers, videos and photos, public comments, and extensive press coverage.

The matrix below indicates that significant irregularities occurred across all six battleground states and across all six dimensions of election irregularities. This finding lends credence to the claim that the election may well have been stolen from President Donald J. Trump.

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Outright Voter Fraud	✓	✓	*	✓	*	✓
Ballot Mishandling		✓	✓	✓	✓	✓
Contestable Process Fouls	✓	✓	✓	✓	✓	✓
Equal Protection Clause Violations	✓	✓	✓	✓	✓	✓
Voting Machine Irregularities	✓	✓	✓	✓	✓	*
Significant Statistical Anomalies	✓	✓	✓	✓		✓

✓ = Wide-Spread Evidence * = Some Evidence

From the findings of this report, it is possible to infer what may well have been a coordinated strategy to effectively stack the election deck against the Trump-Pence ticket. Indeed, the observed patterns of election irregularities are so consistent across the six battleground states that they suggest a coordinated strategy to, if not steal the election outright, strategically game the election process in such a way as to "stuff the ballot box" and unfairly tilt the playing field in favor of the Biden-Harris ticket. Topline findings of this report include:

- The weight of evidence and patterns of irregularities are such that it is irresponsible for anyone – especially the mainstream media – to claim there is "no evidence" of fraud or irregularities.

- The ballots in question because of the identified election irregularities are more than sufficient to swing the outcome in favor of President Trump should even a relatively small portion of these ballots be ruled illegal.

- All six battleground states exhibit most, or all, six dimensions of election irregularities. However, each state has a unique mix of issues that might be considered "most important." To put this another way, all battleground states are characterized by the same or similar election irregularities; but, like Tolstoy's unhappy families, each battleground state is different in its own election irregularity way.

- This was theft by a thousand cuts across six dimensions and six battleground states rather than any one single "silver bullet" election irregularity.

- In refusing to investigate a growing number of legitimate grievances, the anti-Trump media and censoring social media are complicit in shielding the American public from the truth. This is a dangerous game that simultaneously undermines the credibility of the media and the stability of our political system and Republic.

- Those journalists, pundits, and political leaders now participating in what has become a Biden Whitewash should acknowledge the six dimensions of election irregularities and conduct the appropriate investigations to determine the truth about the 2020 election. If this is not done before Inauguration Day, we risk putting into power an illegitimate and illegal president lacking the support of a large segment of the American people.

- The failure to aggressively and fully investigate the six dimensions of election irregularities assessed in this report is a signal failure not just of our anti-Trump mainstream media and censoring social media but also of both our legislative and judicial branches.

    - Republican governors in Arizona and Georgia together with Republican majorities in both chambers of the State Legislatures of five of the six battleground states – Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin[2] – have had both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so – and thereby failed both their states and this nation as well as their party.

    - Both State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to appropriately adjudicate the election irregularities that have come before them. Their failures pose a great risk to the American Republic.

- If these election irregularities are not fully investigated prior to Inauguration Day and thereby effectively allowed to stand, this nation runs the very real risk of never being able to have a fair presidential election again – with the down-ballot Senate races scheduled for January 5 in Georgia an initial test case of this looming risk.

I. Introduction

At the stroke of midnight on Election Day, President Donald J. Trump appeared well on his way to winning a second term. He was already a lock to win both Florida and Ohio; and no Republican has ever won a presidential election without winning Ohio while only two Democrats have won the presidency without winning Florida.[3]

At the same time, the Trump-Pence ticket had substantial and seemingly insurmountable leads in Georgia, Pennsylvania, Michigan, and Wisconsin. If these leads held, these four key battleground states would propel President Trump to a decisive 294 to 244 victory in the Electoral College.

Shortly after midnight, however, as a flood of mail-in and absentee ballots began entering the count, the Trump red tide of victory began turning Joe Biden blue. As these mail-in and absentee ballots were tabulated, the President's large leads in Georgia, Pennsylvania, Michigan, and Wisconsin simply vanished into thin Biden leads.

At midnight on the evening of November 3, and as illustrated in Table 1, President Trump was ahead by more than 110,000 votes in Wisconsin and more than 290,000 votes in Michigan. In Georgia, his lead was a whopping 356,945; and he led in Pennsylvania by more than half a million votes. By December 7, however, these wide Trump leads would turn into razor thin Biden leads – 11,779 votes in Georgia, 20,682 votes in Wisconsin, 81,660 votes in Pennsylvania, and 154,188 votes in Michigan.

Table 1: A Trump Red Tide Turns Biden Blue

	GEORGIA	PENNSYLVANIA	MICHIGAN	WISCONSIN
Trump Lead Midnight 11/3	356,945	555,189	293,052	112,022
Biden "Lead" 12/15	11,779	81,660	154,188	20,682

Sources: Associated Press & Edison/Decision Desk HQ
*Midnight based on state's time zone

There was an equally interesting story unfolding in Arizona and Nevada. While Joe Biden was ahead in these two additional battleground states on election night – by just over 30,000 votes in Nevada and less than 150,000 votes in Arizona – internal Trump Campaign polls predicted the President would close these gaps once all the votes were counted. Of course, this never happened.

In the wake of this astonishing reversal of Trump fortune, a national firestorm has erupted over the fairness and integrity of one of the most sacrosanct institutions in America – our presidential election system. Critics on the Right and within the Republican Party – including President Trump himself – have charged that the election was stolen. They have backed up these damning charges with more than 50 lawsuits,[4] thousands of supporting affidavits and declarations, and seemingly incriminating videos, photos, and first-hand accounts of all manner of chicanery.[5]

Critics on the Left and within the Democrat Party have, on the other hand, dismissed these charges as the sour grapes of a whining loser. Some of these critics have completely denied any fraud, misconduct or malfeasance altogether. Others have acknowledged that while some election irregularities may have existed, they strenuously insist that these irregularities are not significant enough to overturn the election.

There is a similar Battle Royale raging between large anti-Trump segments of the so-called "mainstream" media and alternative conservative news outlets. Across the anti-Trump mainstream media diaspora – which includes most prominently print publications like the New York Times and Washington Post and cable TV networks like CNN and MSNBC – a loud chorus of voices has been demanding that President Trump concede the election.

These same anti-Trump voices have been equally quick to denounce or discredit anyone – especially anyone within their own circle – that dares to investigate what may well turn out to be THE biggest political scandal in American history. Social media outlets like Facebook, Twitter, and YouTube likewise have been actively and relentlessly censoring anyone who dares to call the results of the election into question.

In contrast, alternative news outlets, primarily associated with the American conservative movement, have provided extensive, in-depth coverage of the many issues of fraud, misconduct, and other irregularities that are coming to light. From Steve Bannon's War Room Pandemic[6] and John Solomon's Just the News[7] to Raheem Kassam's National Pulse,[8] to Newsmax,[9] and One America News Network,[10] Americans hungry for facts and breaking developments have been able to find such critical information only by following this alternative coverage.

That the American public is not buying what the Democrat Party and the anti-Trump media and social media are selling is evident in public opinion polls. For example, according to a recent Rasmussen poll: "Sixty-two percent (62%) of Republicans say it is 'Very Likely the Democrats stole the election'" while 28% of Independents and 17% of Democrats share that view.[11]

If, in fact, compelling evidence comes to light proving the election was indeed stolen after a *fait accompli* Biden inauguration, we as a country run the very real risk that the very center of our great American union will not hold.

To put this another way, if the greatest democracy in world history cannot conduct a free and fair election, and if much of the mainstream media of this country won't even fully investigate what is becoming a growing mountain of evidence calling into question the election result, there is little chance that our democracy and this Republic will survive as we know it. It is therefore critical that we get to the bottom of this matter. That is the purpose of this report.

II. Six Dimensions of Election Irregularities across Six Battleground States

This report assesses the fairness and integrity of the 2020 presidential election across six key battleground states where the Democrat candidate Joe Biden holds a slim lead, and the results continue to be hotly contested. As documented in the extensive endnotes, the evidence used to conduct this assessment includes more than 50 lawsuits and judicial rulings, thousands of affidavits and declarations, testimony presented in a variety of state venues, published reports and analyses by think tanks and legal centers, videos and photos, public comments and first-hand accounts, and extensive press coverage.

From a review and analysis of this evidence, six major dimensions of alleged election irregularities have been identified and assessed on a state-by-state basis across six key battleground states: Arizona, Georgia, Michigan, Nevada, Pennsylvania, and Wisconsin. These six dimensions include outright voter fraud, ballot mishandling, contestable process fouls, Equal Protection Clause violations, voting machine irregularities, and significant statistical anomalies.

The matrix in Table 2 provides an overview of the presence or absence of each of the six dimensions of alleged election irregularities in each of the six battleground states. Column 1 lists each of the six dimensions along with the alleged Biden victory margin and the possible illegal ballots due to election irregularities. Columns 2 through 7 in the matrix then indicate the presence or absence of the election irregularities in any given state.

Note that a checkmark in matrix cell indicates there is *widespread* evidence in a given state for a particular dimension of election irregularity while a star indicates there is at least *some* evidence.

Table 2: 2020 Alleged Election Irregularities across the Six Battleground States

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Outright Voter Fraud	✓	✓	*	✓	*	✓
Ballot Mishandling		✓	✓	✓	✓	✓
Contestable Process Fouls	✓	✓	✓	✓	✓	✓
Equal Protection Clause Violations	✓	✓	✓	✓	✓	✓
Voting Machine Irregularities	✓	✓	✓	✓	✓	*
Significant Statistical Anomalies	✓	✓	✓	✓		✓
Biden "Victory" Margin	10,457	11,779	154,188	33,596	81,660	20,682
Possible Illegal Ballots	>100,000	>400,000	Unknown	>100,000	>600,000	>200,000

✓ = Wide-Spread Evidence * = Some Evidence

Two key points stand out immediately from the matrix. First, significant irregularities appear to be ubiquitous across the six battleground states. Only Arizona is free of any apparent widespread ballot mishandling while only Pennsylvania lacks significant statistical anomalies. The rest of the matrix in Table 2 is a sea of checkmarks and occasional stars.

Second, if one compares the alleged Biden victory margin in Column 7 of the figure with the possible illegal ballots in Column 8, it should be clear that the number of possible illegal ballots dwarfs the alleged Biden victory margin in five of the six states.

For example, the alleged Biden victory margin in Nevada is 33,596 votes yet the number of ballots in question is more than three times that. In Arizona, which has the narrowest alleged Biden victory margin at 10,457 votes, there are nearly 10 times that number of possible illegal ballots; and the ratio of the alleged Biden vote lead to possible illegal ballots is even higher for Georgia.

Only Michigan is the exception to the rule. This is not because it is likely to be a true exception but simply because there remains insufficient estimates of how the various types of irregularities in Michigan translate into possible illegal votes.

Clearly, based on this matrix, the American people deserve a definitive answer as to whether this election was stolen from Donald J. Trump. Absent a thorough investigation prior to Inauguration Day, a cloud and a stain will hang over what will be perceived by many Americans as an illegitimate Biden administration.

The next six sections of this report examine in more detail each of the six dimensions of alleged election irregularities.

III. Outright Voter Fraud

Outright voter fraud ranges from the large-scale manufacturing of fake ballots, bribery, and dead voters to ballots cast by ineligible voters such as felons and illegal aliens, ballots counted multiple times, and illegal out-of-state voters. Table 3 provides an overview across the six battleground states of the various types of outright voter fraud that have been alleged to be present.

Table 3: Outright Voter Fraud in the 2020 Presidential Election

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Bribery	✓			✓		
Fake Ballot Manufacturing & Destruction of Legally Cast Real Ballots	✓	✓		*	*	
Indefinitely Confined Voter Abuses		*			*	✓
Ineligible Voters & Voters Who Voted in Multiple States	✓	✓		✓		
Dead Voters & Ghost Voters	✓	✓	*	✓	*	
Counting Ballots Multiple Times			*	*	*	✓
Illegal Out-of-State Voters	✓	✓		✓	*	

✓ = Wide-Spread Evidence * = Some Evidence

From the figure, we see that different types of fraud may be present in all six states. Let's more precisely define each of these different types of fraud using examples that are designed to be illustrative rather than exhaustive.

Bribery

In a voter fraud context, *bribery* refers to the corrupt solicitation, acceptance, or transfer of value in exchange for official action, such as voter registration or voting for a preferred candidate.[12] At least in Nevada, there is a slam dunk case that such bribery occurred.

What is so stunning about the Nevada case is the brazen disregard for our federal bribery laws. In the Silver State, in an effort orchestrated by the Biden campaign, Native Americans appear to have traded their votes not for pieces of silver but rather for Visa gift cards, jewelry, and other "swag."[13] According to the Epoch Times, such vote buying schemes also may have occurred in eight other states, including Arizona and Wisconsin.[14]

Fake Ballot Manufacturing and Destruction of Legally Cast Real Ballots

Fake ballot manufacturing involves the fraudulent production of ballots on behalf of a candidate; and one of the most disturbing examples of possible fake ballot manufacturing involves a truck driver who has alleged in a sworn affidavit that he picked up large crates of ballots in New York and delivered them to a polling location in Pennsylvania.[15] There may be well over 100,000 ballots involved, enough fake ballots alone to have swung the election to Biden in the Keystone State.

Likewise in Pennsylvania, there is both a Declaration and a photo that suggests a poll worker used an unsecured USB flash drive to dump an unusually large cache of votes onto vote tabulation machines. The resultant tabulations did not correlate with the mail-in ballots scanned into the machines.[16]

Arguably the most flagrant example of possible fake ballot manufacturing on behalf of Joe Biden may have occurred at the State Farm Arena in Atlanta, Georgia. The possible perpetrators were caught *in flagrante delicto* on surveillance video.

In one version of this story, poll watchers and observers as well as the media were asked to leave in the middle of the night after a suspicious water leak. Once the room was cleared, several election officials pulled out large boxes of ballots from underneath a draped table. They then proceeded to tabulate a quantity of fake manufactured ballots estimated to be in the range of tens of thousands.[17] Note that a large surge in Biden votes following the tabulation of these ballots can be clearly observed after these votes were processed.[18]

Despite what appears to be damning evidence of a possible crime, a spate of stories appeared across the anti-Trump media diaspora dismissing any concerns. According to these whitewash stories, these were regular and authorized ballot boxes, observers in the media were not asked to leave but simply left on their own, and it is perfectly acceptable to count ballots in the absence of observers.[19] Or so the spin goes.

Of course, this is precisely the kind of incident that should be fully investigated both by Georgia's Attorney General as well as by the Federal Department of Justice. Yet it remains unclear as to whether such investigations are underway. Meanwhile, the videotape itself, absent an adequate explanation, has contributed to the current climate of skepticism surrounding the fairness and integrity of the election.

Finally, as an example of the possible *destruction of legally cast real ballots* there is this allegation from a court case filed in the United States District Court for the District of Arizona: Plaintiffs claim that over 75,000 absentee ballots were reported as unreturned when they were actually returned. These absentee ballots were then either lost or destroyed (consistent with allegations of Trump ballot destruction) and/or were replaced with blank ballots filled out by election workers or other third parties.[20]

Indefinitely Confined Voter Abuses

Indefinitely confined voters are those voters unable to vote in person because of old age or some disability. There are two types of possible abuses associated with such indefinitely confined voters.

The first kind of abuse involves exploiting the elderly or the infirm by effectively hijacking their identities and votes. For example, in Georgia, the family of an elderly man in a nursing home facility discovered that a mail-in ballot had been requested and submitted under his voter registration identity, yet it was done without his consent.[21] In a similar situation in Pennsylvania, two parents and their daughter who has Downs Syndrome went to vote in person and discovered that a mail-in ballot had both been requested and submitted for the daughter without her consent.[22]

The second kind of indefinitely confined voter abuse is far more consequential, at least in the state of Wisconsin. The key allegation here in several court filings is that "bad-faith voters" registering as "indefinitely confined" intentionally broke "Wisconsin election law to circumvent election integrity photo identification requirements." In a nutshell, they were able to vote without showing a voter identification photo and therefore underwent a far less rigorous I.D. check than would otherwise have been conducted.

This abuse happened, according to one press account, after "clerks in Dane and Milwaukee counties offered illegal advice that encouraged individuals to use indefinite confinement as a way to ignore the state's photo I.D. requirement."[23] The Trump side has called this correctly an open invitation to fraud; and stories and pictures abound of Wisconsin voters who registered as indefinitely confined but were seen also attending weddings, riding their bikes, going on vacation, and otherwise be anything but confined.[24]

Here is what is most important about this particular type of election fraud: In the wake of the expanded definition of indefinitely confined voters – a definition ruled legally *incorrect* by the Wisconsin Supreme Court[25] – the number of indefinitely confined voters surged from just under 70,000 voters in 2019 to over 200,000 in 2020.[26] This 130,000 vote increment of new indefinitely confined voters is more than five times the Biden victory margin in Wisconsin.

Ineligible Voters and Voters Who Voted in Multiple States

Ineligible voters include felons deemed ineligible, underage citizens, nonregistered voters, illegal aliens, illegal out-of-state voters, and voters illegally using a post office box as an address.[27]

In a court filing by the Trump campaign legal team, lead counsel Ray Smith provided a list of more than 70,000 allegedly ineligible voters casting ballots in Georgia in the 2020 election.[28] Also in Georgia, over 20,000 people appear to have filed a Notice of Changed Address form to the Georgia state government or had other indications of moving out of state. Yet, these clearly ineligible out-of-state voters appeared to have remained on the voter rolls and voted in the 2020 election.[29]

As additional data points regarding ineligible out-of-state voters, there are these: Between 80 and 100 self-proclaimed Black Lives Matter-affiliated members from other states have admitted to having voted in Pennsylvania.[30]

As for those *voters who vote in multiple states*, one lawsuit claims that roughly 15,000 mail-in or absentee ballots were received in Nevada from voters who were known to have voted in other states.[31] It is useful to note here that in Nevada, poll workers allegedly were not consistent in their procedures when checking voters in to vote about whether they accepted California or Nevada Voter Identification as proof of eligibility to register to vote.[32]

Dead Voters and Ghost Voters

According to widespread evidence, there was a surprising number of ballots cast across several key battleground states by deceased voters, sparking one wag to quip, in reference to a classic Bruce Willis movie, this was the "Sixth Sense" election – I see dead people voting.

In Pennsylvania, for example, a statistical analysis conducted by the Trump Campaign matching voter rolls to public obituaries found what appears to be over 8,000 confirmed dead voters successfully casting mail-in ballots.[33] In Georgia – underscoring the critical role any given category of election irregularities might play in determining the outcome – the estimated number of alleged deceased individuals casting votes almost exactly equals the Biden victory margin.

In Michigan, according to one first-hand account offered in a declaration, computer operators at a polling location in Detroit were manually adding the names and addresses of thousands of ballots to vote tabulation systems with voters who had birth dates in 1900.[34] And in Nevada, a widower since 2017 saw that his deceased wife had successfully cast a mail-in ballot on November 2, 2020, three and a half years after her death. [35]

It may be useful to note here that dead voters played a critical role in stealing the election from Richard Nixon, a theft orchestrated by Mayor Richard Daley and his Chicago political machine. According to one report "more than 3,000 votes [were] cast in the names of individuals who were dead, and more than 31,000 individuals voted twice in different locations in the city." President Kennedy's victory margin in Illinois was less than 9,000 votes.

On the Ghost Voter front, a "Ghost Voter" is a voter who requests and submits a ballot under the name of a voter who no longer resides at the address where that voter was registered. In Georgia for example, it is alleged that over 20,000 absentee or early voters – almost twice the Biden victory margin – cast their ballots after having moved out of state.[36] In Nevada, a poll worker reported that there were as many as 50 ballots per day being delivered to homes vacated by their former residents.[37]

Counting Ballots Multiple Times

Counting ballots multiple times occurs most egregiously when batches of ballots are repeatedly rescanned and re-tabulated in electronic voting machines. It can also happen when the same person votes multiple times within the same day. Evidence of these particular kinds of "ballot stuffing" are present across all six battleground states.

For example, in Wisconsin, poll workers were observed running ballots through tabulation machines more than once.[38] In Wayne County, Michigan, Republican poll watchers observed canvassers re-scanning batches of ballots through vote tabulation machines up to 3 to 4 times.[39]

In Pennsylvania, a poll worker observed a woman vote twice in the same day by changing her appearance.[40] Another poll worker observed people in voting lines in one corner of a polling location voting, and then coming to another polling location at the other side of the building to vote.[41] Still another poll worker witnessed a woman voting twice at voting machines on Election Day.[42]

IV. Ballot Mishandling

Ballot mishandling represents the second major dimension of alleged election irregularities in the 2020 presidential election. As Table 4 illustrates, this is a multifaceted problem across the battleground states. Let's work our way through this figure starting with the failure to properly check the identification of voters.

Table 4: Ballot Mishandling in the Battleground States

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
No Voter I.D. Check			*	*		✓
Signature Match Check Abuses		✓		✓	✓	
"Naked Ballots" Lacking Outer Envelope			*		✓	
Broken Chain of Custody & Unauthorized Ballot Handling or Movements		✓	✓	✓	✓	✓
Ballots Accepted Without Postmarks & Backdating of Ballots			*			*

✓ = Wide-Spread Evidence * = Some Evidence

No Voter I.D. Check

It is critical for the integrity of any election for poll workers to properly verify a voter's identity and registration when that voter comes in to cast an in-person ballot. However, there is at least some evidence of a lack of adequate voter ID check across several of the battleground states.

For example, in Michigan, the chairperson of a polling location permitted an individual to vote without presenting voter identification and another with only a photocopy of a driver's license.[43]

In Nevada, poll workers were instructed to advise people who wanted to register to vote and did not have proper Nevada IDs or Driver's Licenses to do the following: These unregistered voters could go outside into the parking lot and make an appointment with the Department of Motor Vehicles as late as January 2021 to obtain a Nevada Driver's License as proof of their identity. They could then bring in confirmation of their DMV appointment in either paper or digital form; and that would be sufficient to allow them to be registered.[44]

Signature Matching Abuses

It is equally critical that ballot counters legally verify mail-in and absentee ballots by checking if the signatures on the outer envelopes match the voters' registration records.[45] Note, however, that a variety of signature matching abuses represent a major issue in Nevada, Pennsylvania, and especially in Georgia.

In Georgia, contrary to state law, the Secretary of State entered into a Consent Decree with the Democrat Party that weakened signature matching to just one verification instead of two. This illegal weakening of the signature match test has called into question more than 1.2 million mail-in ballots cast in Georgia.[46]

Georgia is not the only state where signature match check abuses have surfaced. Nevada law requires that *persons* – not machines – review all signatures and ballots. Yet the Clark County Registrar of Voters used a defective signature matching computer system called Agilis to conduct such checks.[47] As will be discussed further below, this problem of machines replacing humans contrary to Nevada state law was compounded by the fact that the Agilis system has an unacceptably low accuracy rate, making it easier for illegal ballots to slip through its screen.[48]

Signature match abuses also surfaced in Wisconsin where mandatory voter information certifications for mail-in ballots were reduced and/or eliminated, again contrary to state law. As noted in one lawsuit, this change "undermined the authority of the state legislature, reduced the security and integrity of the election by making it easier to engage in mail-in ballot fraud and created another standard-less rule in conflict with the clear terms of the Wisconsin Election Code, preventing uniform treatment of absentee ballots throughout the State."[49]

"Naked Ballots" Lacking Outer Envelope

A *naked ballot* is a mail-in or absentee ballot lacking an outer envelope with the voter's signature on it. It is illegal to accept the naked ballot as the outer envelope provides the only way to verify a voter's identity.

The illegal acceptance of naked ballots appears to be particularly acute in Pennsylvania as a result of ill-advised "guidance" issued by the Secretary of State – a registered Democrat[50] – that such naked ballots be counted.

This issuance of such guidance, in violation of state law,[51] appears to be a blatant attempt by a Democrat politician to boost the count for Joe Biden as it was clear that Democrats would be voting disproportionately higher through mail-in ballots. This incident is especially egregious because when the Pennsylvania Supreme Court rejected this guidance, the Secretary of State refused to issue new guidance directing election officials to NOT count non-compliant mail-in or absentee ballots.[52]

Broken Chain of Custody & Unauthorized Ballot Handling or Movements

The maintenance of a proper chain of custody for ballots cast is the linchpin of fair elections. Chain of custody is broken when a ballot is fraudulently transferred, controlled, or moved without adequate supervision or oversight.[53]

While chain of custody issues can apply to all ballots, the risk of a broken chain of custody is obviously higher for mail-in and absentee ballots. This is because the ballots have to go through more hands.

In the 2020 presidential election, the increased use – often illegal use – of unsupervised drop boxes arguably has enhanced the risk of a broken chain of custody. So, too, has the increased practice of so-called "ballot harvesting" whereby third parties pick up ballots from voters and deliver them to drop boxes or directly to election officials.

Both drop boxes and ballot harvesting provide opportunities for bad actors to insert fraudulent ballots into the election process. That this is a very serious matter is evident in this observation by BlackBoxVoting.org: "In court cases, chain of custody violations can result in refusal to admit evidence or even throwing a case out. In elections, chain of custody violations can result in 'incurable uncertainty' and court orders to redo elections."[54] (emphasis added)

As an example of the drop box problem, in Pennsylvania, ballots were illegally dumped into drop boxes at the Nazareth ballot drop center in violation of state law.[55] Likewise in Pennsylvania, a man caught on videotape and photos came out of an unmarked Jeep extracting ballots from an unsupervised ballot drop-box to bring them into a ballot counting center. That same man was observed to come back with an empty ballot container to place in the unsupervised drop box.[56]

In Wisconsin, the state's Election Committee illegally positioned five hundred drop boxes for collection of absentee ballots across the state. However, these drop boxes were disproportionately located in urban areas which tend to have much higher Democrat registration, thereby favoring the candidacy of Joe Biden. Note: Any use of a drop box in Wisconsin is illegal by statute. Therefore, the votes cast through them cannot be legally counted in any certified election result.[57]

As an example of ballot harvesting – in this case at the front end of the process – 25,000 ballots were requested from nursing home residents in Pennsylvania at the same time.[58]

As additional examples of a possible broken chain of custody, there are these: Large bins of absentee ballots arrived at the Central Counting Location in Wisconsin with already opened envelopes, meaning that ballots could have been tampered with.[59] They were nonetheless counted.

Also in Wisconsin, an election worker was observed moving bags of blank ballots into a vehicle and then driving off without supervision.[60] There is also the previously referenced case whereby a truck driver has offered a firsthand account of moving large quantities of fake manufactured ballots from New York to Pennsylvania.

As a final note on the unauthorized handling or movement of ballots, there is the problem of *illegal ballot counters*. These are persons who not legally permitted and/or certified to be counting ballots.

In one curious case, an individual who worked as an official photographer for Kamala Harris' campaign in 2019[61] was alleged to be involved in scanning ballots in Floyd County, Georgia. Ballot counters cannot have any ties to candidates in a presidential election.

Ballots Accepted Without Postmarks and Backdating of Ballots

Across all of the battleground states, it is against state law for poll workers to count either mail-in or absentee ballots that lack postmarks. It is also illegal to backdate ballots so that they may be considered as having met the election deadline for the receipt and counting of such ballots. There is some evidence of these irregularities in several of the battleground states.

For example, in Wisconsin, according to one Declaration, employees of the United States Postal Service (USPS) in Milwaukee were repeatedly instructed by two managers to backdate late-arriving ballots so they could still be counted.[62] In addition, the USPS was alleged to have backdated as many as 100,000 ballots in Wisconsin.[63]

Similarly, in Detroit, Michigan, as noted in a court case, poll workers were instructing ballot counters to backdate absentee ballots so they could be counted.[64] One poll watcher also observed ballots in Michigan being run through vote tabulation machines without postmarks on them.[65]

V. Contestable Process Fouls

Contestable process fouls represent the third dimension of election irregularities in the 2020 presidential election. The various forms such process fouls can take are illustrated in Table 5 across the six battleground states.

Table 5: Contestable Process Fouls in the Battleground States

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Abuses of Poll Watchers & Observers	✓	✓	✓	✓	✓	✓
Mail-In & Absentee Ballot Rules Violated Contrary to State Law		✓			✓	✓
Voters Not Properly Registered Allowed to Vote		✓	*	✓	*	✓
Illegal Campaigning at Poll Locations			*		*	*
Ballots Cured by Poll Workers or Voters Contrary to Law	✓	✓	✓	✓	✓	✓

✓ = Wide-Spread Evidence * = Some Evidence

Abuses of Poll Watchers and Observers

Central to the fairness and integrity of any election is the processes by which observers monitor the receipt, opening, and counting of the ballots. You can see in the Table 5 that poll watcher and observer abuses were present across all six battleground states.

In Georgia,[66] Michigan,[67] and Pennsylvania,[68] poll watchers and observers were denied entry to ballot counting centers by Judges of Elections and other poll workers. This was despite presenting proper certification and identification.

In Georgia,[69] Michigan,[70] Nevada,[71] and Pennsylvania,[72] Republican poll watchers were also forced inside confined areas, thereby limiting their view. In some cases, this confinement was enforced by local law enforcement.

Across these four battleground states, Republican poll watchers were also directed to stand at unreasonably lengthy distances from ballot counters. In Michigan – arguably the "first among equals" when it comes to observer abuses – poll workers put up poster boards on the windows of the room where ballots were being processed and counted so as to block the view.[73] In Pennsylvania, tens of thousands of ballots were processed in back rooms where poll observers were prohibited from being able to observe at all.[74]

This is an extremely serious matter because it is these poll watchers and observers who represent the frontline defenders of a fair election process. Their job is to make sure all ballots are handled properly and tabulated accordingly. They seek to answer questions like: Is there a signature match process being conducted? Does each ballot have an outer envelope or is it a naked ballot? Are ballots being run more than once through the tabulation machines?

When poll watchers or observers are barred from viewing or forced to view from unacceptably large distances, these watchdogs cannot accurately answer these questions. They, therefore, cannot fulfill their critical watchdog function.

Mail-In Ballot and Absentee Ballot Rules Violated Contrary to State Law

In Georgia, more than 300,000 individuals were permitted to vote who had applied for an absentee ballot more than 180 days prior to the Election Day. This is a clear violation of state law.[75]

In both Pennsylvania and Wisconsin, Democrat election officials acted unilaterally to accept both mail-in and absentee ballots after Election Day. State Republicans have argued this is contrary to state law.

In Pennsylvania, absentee and mail-in ballots were accepted up to three days after Election Day.[76] On November 7th, in anticipation of a legal challenge, the United States Supreme Court ordered that the approximately 10,000 absentee and mail-in ballots that had arrived past November 3rd be separated from ballots that had arrived on Election Day.[77] This direction notwithstanding, a poll watcher reported on November 7th that, in Delaware County, ballots received the previous night were not being separated from ballots received on Election Day, contrary to state law.[78]

Wisconsin state law does not permit early voting. Nonetheless, city officials in the Democrat stronghold of Madison, Wisconsin assisted in the creation of more than 200 "Democracy in the Park" illegal polling places.

These *faux* polling places were promoted and supported by the Biden campaign. They provided witnesses for absentee ballots and acted in every way like legal polling places. Moreover, they received ballots outside of the limited 14-day period preceding an election that is authorized by statute for in-person or absentee balloting. These were clear violations of state law.[79]

Voters Not Properly Registered Allowed to Vote

One of the jobs of poll workers is to ensure that in-person voters are legally registered and are who they say they are. Across at least three of the six battleground states – Georgia, Nevada, and Wisconsin – this job may not have been effectively done.

In Wisconsin, for example, officials refused to allow poll watchers to challenge the qualifications of people applying to vote or require proof of such persons' qualifications.[80] In Georgia, more than 2,000 individuals appear to have voted who were not listed in the State's records as having been registered to vote.[81]

In Pennsylvania, a poll watcher observed poll workers taking individuals whose names did not appear in voter registration books back into a separate area that was unobserved by any poll watchers. There, these apparently unregistered voters met with a Judge of Elections who allegedly told them: "you go back in, tell them this is your name, and you can vote."[82]

Illegal Campaigning at Poll Locations

Poll workers are supposed to remain politically neutral. When a poll worker displays bias for one political candidate over another at a polling location, this is contrary to state law. Unfortunately, this law appears to have been repeatedly violated in Michigan, Pennsylvania, and Wisconsin.

For example, in Pennsylvania, poll workers were wearing paraphernalia from a group called "Voter Protection." This is a 100% Democrat-funded Political Action Committee dedicated to Democrat redistricting in Pennsylvania; and the wearing of its paraphernalia constitutes illegal campaigning at the polls.[83]

In a similar type of illegal campaigning in Michigan, poll workers were allowed to wear Black Lives Matter shirts and were seen carrying tote bags of President Obama paraphernalia.[84] In addition, poll workers with Biden and Obama campaign shirts on were allowed on the ballot counting floor.[85]

In Wisconsin, representatives from the Biden campaign were outside with clipboards talking to voters on their way in to vote. They were clearly inside the prohibited perimeter for electioneering. Poll workers did nothing to address this illegal campaigning despite the objections of observers.[86]

Ballots Cured by Poll Workers or Voters Contrary to Law

Under prescribed circumstances, both poll workers and voters may fix ballots with mistakes or discrepancies. This process is known as "ballot curing."

In nineteen states, poll workers must notify voters if there are errors or discrepancies on their ballots and allow them to "cure" or correct any errors so their votes will count.[87] However, in states that do not allow curing, ballots with discrepancies such as missing or mismatched signatures must be discarded.[88]

In Pennsylvania, and contrary to state law, poll workers were trained to allow voters to cure or "correct" their ballots.[89] According to one court filing, Democrat-controlled counties in Pennsylvania participated in pre-canvass activities prior to Election Day "by reviewing received mail-in ballots for deficiencies."[90] Such discrepancies included "lacking the inner secrecy envelope or lacking a signature of the elector on the outer declaration envelope." Voters were then notified so that they could cure their ballots – a clear violation of state law.[91]

Numerous other examples of illegally cured ballots abound. For example, in Wisconsin, tens of thousands of ballots were observed to be corrected or cured despite election observer objections.[92]

In Pennsylvania, poll workers sorted approximately 4,500 ballots with various errors into bins. Poll workers then re-filled out the 4,500 ballots so that they could be read by tabulation machines, an action contrary to state law.[93]

In Michigan, poll workers altered the dates on the outer envelopes of the ballots so that they would be able to count them.[94] Michigan poll workers also filled out blank ballots to "correct" mail-in and absentee ballots according to what they believed the "voter had intended."[95]

VI. Equal Protection Clause Violations

The Equal Protection Clause is part of the 14th Amendment of the U.S. Constitution and a fundamental pillar of the American Republic. This Equal Protection Clause mandates that no State may deny its citizens equal protection of its governing laws.[96]

Table 6 illustrates three major alleged violations of the Equal Protection Clause in the 2020 presidential election. As the table illustrates, each violation was observed to occur across all six battleground states.

Table 6: Equal Protection Clause Violations in the Six Battleground States

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Higher Standards of Certification & I.D. Verification Applied to In-Person Voters	✓	✓	✓	✓	✓	✓
Different Standards of Ballot Curing	✓	✓	✓	✓	✓	✓
Differential & Partisan Poll Watcher Treatment	✓	✓	✓	✓	✓	✓

✓ = Wide-Spread Evidence * = Some Evidence

Higher Standards of Certification & I.D. Verification Applied to In-Person Voters

The first alleged violation focuses on the application of higher standards of certification and voter identification for in-person voters than mail-in and absentee ballot voters. In effect, these higher standards disproportionately benefited the candidacy of Joe Biden because President Trump had a much higher percentage of in-person voters than mail-in and absentee voters. Indeed, mail-in and absentee ballots were largely skewed for Joe Biden across the country by ratios as high as 3 out of 4 votes in some states.[97]

Note here that much of the alleged fraud and ballot mishandling focused on mail-in voters and absentee ballots. Therefore, the lower the level of scrutiny of these voters, the more illegal votes for Joe Biden relative to Donald Trump could slip in. It should likewise be noted here that this particular violation of the Equal Protection Clause was further enabled by poll watchers being denied meaningful observation.
Perhaps the most egregious examples of this particular violation of the Equal Protection clause occurred in Georgia and Michigan. Georgia, for example, requires ID for voting in-person and Michigan will only allow provisional voting without an ID. However, in both Georgia and Michigan, a valid ID is not required to vote by mail so long as the person has already registered in a previous election.

These procedures are ripe for fraud. In fact, there is evidence that election fraudsters targeted voters who had voted in past elections but not voted in more recent ones. These fraudsters could then cast ballots on behalf of these infrequent voters with little likelihood they would be caught. Numerous affidavits, however, detail persons arriving to vote at polls only to be informed that records indicate they had already voted. At least fourteen such affidavits have been made by Georgians.

As a further example, in Wisconsin, mail-in ballots were accepted without witness signatures placed properly in the allocated envelope location.[98] A comparable process for in-person voting would have resulted in the invalidation of the vote.

Different Standards of Ballot Curing

As a second major violation of the Equal Protection Clause, likewise observed across all six battleground states, different standards for correcting mistakes on ballots (ballot curing) were applied across different jurisdictions within the states. Often, jurisdictions with predominantly Democrat registration were more expansive about allowing the curing of ballots than jurisdictions with predominantly Republican registration.

In Pennsylvania, there was a clear difference between how ballots were – or were not – cured in Republican counties versus Democrat counties. When Pennsylvania's Secretary of State Kathy Boockvar issued illegal guidance authorizing counties to cure ballots, this illegal guidance was not followed in at least eight different Republican counties.[99] Meanwhile, ballots were cured in Democrat counties under this illegal guidance.[100]

In Arizona, there likewise was a clear difference between how in-person voters were treated versus mail-in ballots. On the one hand, mail-in voters had up to 5 days to "cure" or "fix" invalid mail-in ballots sent prior to Election Day.[101] On the other hand, in-person voters in Maricopa County, for example, had to deal with poll workers who did not know how to work electronic voting machines properly. This resulted in thousands of in-person votes being marked incorrectly and disregarded rather than cured.[102]

Differential and Partisan Poll Watcher Treatment

In most states, political party candidates and ballot issue committees are able to appoint poll watchers and observers to oversee the ballot counting process.[103] Such poll watchers and observers must be registered voters and present certification to the Judge of Elections in order to be able to fulfill their duties at a polling location.[104]

Such certified poll watchers should be free to observe at appropriate distances regardless of their party affiliation. Yet in key Democrat strongholds, e.g., Dane County in Wisconsin and Wayne County in Michigan, which yielded high Biden vote counts, Republican poll watchers and observers were frequently subject to different treatment ranging from denial of entry to polling places to harassment and intimidation.

For example, in Georgia, a certified poll watcher witnessed other poll workers at a polling location discussing how they should not speak to her due to her party affiliation. [105] In Pennsylvania, a Republican poll watcher was harassed and removed from the polling location due to his party affiliation.[106] In Wisconsin, a Republican poll watcher was prevented from observing due to the fact that polling locations were not allowing Republicans in.[107]

Note the synergy here between the problem of the process foul involved with denying access to certified poll watchers (discussed in the previous section) and the violation of the Equal Protection Clause such conduct entails when such denial, harassment, and intimidation differs by party affiliation.

VII. 2020 Election Voting Machine Irregularities

Perhaps no device illustrates that technology is a double-edged sword than the machines and associated software that have come to be used to tabulate votes across all 50 states.[108] Types of voting equipment include optical scanners used to process paper ballots, direct recording electronic systems which voters can use to directly input their choices, and various marking devices to produce human-readable ballots.[109]

Two main types of voting machine irregularities have been alleged in the 2020 presidential election. As Table 7 illustrates, these types of irregularities include large-scale voting machine inaccuracies together with inexplicable vote switching and vote surges, often in favor Joe Biden.

Table 7: 2020 Voting Machine Irregularities

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Large-Scale Voting Machine Inaccuracies	✓		✓	✓		
Inexplicable Vote Switching and Vote Surges In Favor of Biden	✓	✓	✓			

✓ = Wide-Spread Evidence * = Some Evidence

Large-Scale Voting Machine Inaccuracies

Much has been made about the shadowy genesis of a company called Dominion which provides voting machines and equipment to 28 states.[110] According to critics, Dominion's roots may be traced to an effort by the Venezuelan dictator Hugo Chavez to rig his sham elections.[111] Dominion is also alleged to have ties to the Clinton Foundation,[112] while the Smartmatic software used in the Dominion machines is alleged to have links to the shadowy anti-Trump globalist financier George Soros.[113]

The controversy swirling over Dominion and Smartmatic notwithstanding, one of the biggest problems with machine inaccuracies may be traced to a company called Agilis. Nevada election officials in Clark County, a Democrat stronghold in Nevada, used Agilis signature verification machines to check over 130,000 mail-in ballot signatures.

According to a court case filed in the First Judicial District Court in Carson City, the Agilis machines used a "lower image quality than suggested by the manufacturer." Clark County Election Department officials also lowered the accuracy rate below the manufacturer's recommendations, making the whole verification process unreliable. [114]

In a test run, it was proven that, at the manufacturer's setting, the Agilis machine already had a high tolerance for inaccuracies—as high as 50% non-matching. In other words, half of the ballots that might be moved through the machine would be impossible to verify; and Clark County officials lowered that threshold even further.[115]

As a final comment on this case, there is also the broader legal matter that the Agilis machines were used to "entirely replace signature verification by election personnel." This is contrary to Nevada state law.

As noted in a court case: "In violation of Nevada law, the Clark County Election Department allows the Agilis machine to solely verify 30% of the signatures accompanying the mail-in ballots without ever having humans inspect those signatures."[116]

A similar problem has been alleged in a court filing in Arizona with a software known as the Novus 6.0.0.0. In cases where ballots were too damaged or illegible to be read by vote tabulation machines, Novus was used in an attempt to cure or restore the ballots. The system would do so by trying to read the applicable scans of the original rejected ballots. However, as noted in a court case filed by Kelli Ward, Chairwoman of the Arizona Republican Party: "the software was highly inaccurate, and it often flipped the vote." [117]

Inexplicable Vote Switching and Vote Surges In Favor of Biden

As a further complication to the Novus software problem in Arizona referenced above, the software was not only highly inaccurate. According to observers, and as an example of inexplicable vote switching, "the software would erroneously prefill 'Biden' twice as often as it did 'Trump.'"[118]

At least one instance of a large and inexplicable vote switching and vote surge in favor of Joe Biden took place in Antrim County, Michigan – and it is associated with the controversial aforementioned Dominion-Smartmatic voting machine hardware-software combo.[119] In this Republican stronghold, 6,000 votes were initially, and incorrectly, counted for Joe Biden. The resulting vote totals were contrary to voter registration and historical patterns and therefore raised eyebrows. When a check was done, it was discovered that the 6,000 votes were actually for Donald J. Trump.

A subsequent forensic audit of the Antrim County vote tabulation found that the Dominion system had an astonishing error rate of 68 percent.[120] By way of comparison, the Federal Election Committee requires that election systems must have an error rate no larger than 0.0008 percent.[121]

Perhaps even more troubling given concerns over hackers and Dominion's alleged ties to bad foreign actors, the records that would have allowed the detection of remote internet access went missing from the Antrim County system. This was in direct violation of Michigan state law,[122] which requires retention of voting records for 22 months -- such information was in place for previous election years, but not this election. At the very least, the results of this audit indicates the need for further investigation of the Dominion system across other states in the country.

In Georgia, there were numerous "glitches" with the Dominion machines where the results would change. The most notable of these changes was a 20,000 vote surge for Biden and 1,000 vote decrease for Trump.[123]

VIII. Statistical Anomalies in the Six Battleground States

The 2020 presidential election appears to feature at least four types of statistical anomalies that raise troubling questions. Table 8 illustrates the incidence of these statistical anomalies across the six battleground states. As you can see from the table, Wisconsin and Georgia are characterized by the highest degree of statistical anomalies, with three of the four anomalies present. Nevada and Arizona show two anomalies present while Michigan has at least one. Let's take a more granular look now at each of these types of statistical anomalies.

Table 8: Statistical Anomalies in the Battleground States

	ARIZONA	GEORGIA	MICHIGAN	NEVADA	PENNSYLVANIA	WISCONSIN
Significant Changes In Absentee Ballot Rejection Rates From Previous Elections		✓		✓	✓	
Excessively High Voter Turnout (at times exceeding 100%)	✓	✓	✓	✓		✓
Statistically Improbable Vote Totals Based on Party Registration & Historical Patterns	✓					✓
Unusual Vote Surges		✓	*			✓

✓ = Wide-Spread Evidence * = Some Evidence

Dramatic Changes in Mail-in and Absentee Ballot Rejection Rates from Previous Elections

It is routine across the 50 states for mail-in-and absentee ballots to be rejected for any number of reasons. These reasons may include: the lack of a signature or adequate signature match, a late arrival past a deadline,[124] the lack of an external envelope that verifies voter-identification (a naked ballot),[125] or if voters provide inaccurate or incomplete information on the ballots.[126]

In the 2020 presidential race, Joe Biden received a disproportionately high percentage of the mail-in and absentee ballots. Perhaps not coincidentally, we saw a dramatic fall in rejection rates in Pennsylvania, Nevada, and especially Georgia.

For example, in Nevada, the overall rejection rate dropped from 1.6%[127] in 2016 to 0.58% in 2020.[128] In Pennsylvania, the 2016 rejection rate of 1.0%[129] dropped to virtually nothing at 0.28%.[130] The biggest fall in the overall absentee ballot rejection rate came, however, in Georgia. Its rejection rate fell from 6.8%[131] in 2016 to a mere 0.34%[132] in 2020.

These dramatically lower rejection rates point to a conscious effort by Democrat election officials across these key battleground states to subject mail-in and absentee ballots to a lower level of scrutiny. That this kind of government conduct and gaming of our election system may have contributed to tipping the scales in favor of Joe Biden can be illustrated in this simple calculation:

In the 2020 race, Georgia election officials received 1,320,154 mail-in and absentee ballots. If these ballots had been rejected at the 2016 rate of 6.8% instead of the 2020 rate of 0.34%, there would have been 81,321 ballots rejected instead of the 4,489 ballots that were actually rejected.

Under the conservative assumption that 60% of these mail-in and absentee ballots went to Joe Biden,[133] this dramatic fall in the rejection rate provided Joe Biden with an additional 16,264 votes. That's more than the margin of the alleged Biden victory in Georgia.

Excessively High Voter Turnout (at times exceeding 100%)

When there are more ballots cast than registered or eligible voters, fraud has likely taken place. During the 2020 presidential election, excessively high voter turnout occurred across all six swing states.

In analyzing this problem, it is important to distinguish between states that have same-day registration and those that don't. States with same-day registration can plausibly have voter turnout that is higher than 100%. However, is impossible for that to happen in states without same-day registration without fraud having taken place.

Consider, then, Arizona which does not allow same-day voter registration. According to testimony from an MIT-trained mathematician, Candidate Biden may have received a weighted 130% total of Democrat votes in Maricopa County to help him win the state due to an algorithm programmed into the Dominion voting machines used there.[134]

Although Michigan does allow same-voter registration, voter turnout was still abnormally high. Here again, the Dominion voting system has been implicated. To wit:

Cybersecurity executive and former NASA analyst, Russ Ramsland, testified that in Wayne County, Michigan, where Dominion Voting Systems equipment was used, 46 out of 47 precincts in the county displayed greater than a 96% voter turnout. 25 out of those precincts showed a 100% voter turnout.[135]

Wisconsin, which also allows same-day voter registration, also reported abnormally high voter turnout when compared to 2016 numbers. For example, Milwaukee reported a record 84% voter turnout during the 2020 presidential election versus 75% in 2016.[136] Of the city's 327 voting wards, 90 reported a turnout of greater than 90%.[137]

Statistically Improbable Vote Totals Based on Party Registration and Historical Patterns

The 2020 presidential election was characterized by strong partisan voting patterns consistent with historical patterns. As a rule, heavily Republican jurisdictions voted heavily for President Trump and heavily Democrat jurisdictions voted heavily for Joe Biden.

In some cases, however, there were instances where these partisan and historical patterns were violated. It is precisely in such instances where either outright fraud or machine inaccuracies or manipulations are most likely to be operative.

As one example of such statistically improbable vote totals, there are the results in Arizona's Fifth Congressional District. In one precinct in the suburb of Queen Creek, the vote percent for President Trump dropped dramatically relative to 2016, from 67.4 to 58.5 percent.[138] This was attributed to an "unusually high" number of duplicate ballots.[139]

Unusual Vote Surges

Several unusual vote surges took place in the very early hours of the morning of November 4th in Georgia, Michigan, and Wisconsin. An analysis conducted by the Voter Integrity Project of *The New York Times* publicly reported data on Election Day that showed several vote "spikes" that were unusually large in size with unusually high Biden-to-Trump ratios. Such spikes or surges could well indicate that fraudulent ballots had been counted.

In Georgia, for example, an update at 1:34 AM on November 4th showed 136,155 additional ballots cast for Joe Biden, and 29,115 additional votes cast for President Trump.[140] An update in Michigan at 3:50 AM on November 4th showed an update of 54,497 additional votes cast for Joe Biden, and 4,718 votes cast for President Trump.[141] And an update in Wisconsin at 3:42 AM on November 4th showed 143,379 additional ballots cast for Joe Biden, and 25,163 votes cast for President Trump.[142]

IX. A State-By-State Analysis and Signal Failure of Our Legislative and Judicial Branches

All happy families are alike; each unhappy family is unhappy in its own way.

– ***Anna Karenina, by Leo Tolstoy***

It should be clear at this point that all six battleground states suffer from most or all of the six dimensions of election irregularities documented in this report. However, like Tolstoy's unhappy families, it is also true that each battleground state is different in its own election irregularity way. That is, each battleground state may be characterized by a unique mix of issues that, impressionistically, might be considered "most important" in swinging that state for Joe Biden.

Consider Arizona, a state with the lowest alleged Biden victory margin at 10,457 votes. This is a state with statistically improbable high voter turnouts in Maricopa and Pima counties; widespread ballot mishandling; and 1.6 million mail-in ballots (which tended towards Biden) subjected to much lower standards of certification and ID verification than in-person voters (who tended towards Trump).

In Georgia, the alleged Biden victory margin was just 11,779 votes. What perhaps jumps out most in the Peach State is the illegal Consent Decree that effectively gutted the signature match requirements for millions of mail-in ballots. There is also the quite unresolved fake ballot manufacturing matter of the roughly 100,000 ballots that were mysteriously pulled, in the dead of night, out from underneath tables and expeditiously tabulated. Of course, we saw that Georgia's electoral version of a Three-card Monte sleight-of-hand led to a strong Biden vote surge.

Of all of the six battleground states which suffered from numerous observer and poll watcher abuses, Michigan must rank as "first among equals." With its "board up the windows" and "rough up the observers" tactics, Detroit in Wayne County was the center of this "see no evil" universe. When two local Republican officials tried to withhold certification of the votes in this county for practices such as these and demanded an audit, they were subject to extreme intimidation and "doxing" and quickly capitulated.[143]

As for Nevada, this is a state likewise with a very narrow alleged victory margin for Joe Biden – 33,596 votes. Here, voting machine irregularities associated with the Agilis machine have called into question as many as 130,000 votes. There may also be an unusually large number of ballots cast by out-of-state voters and others who did not meet residency requirements. Of course, the brazen bribery of Native Americans to vote for Joe Biden is a dark stain on the state and the Democrat Party.[144]

In Pennsylvania, an equally brazen Democrat Secretary of State issued illegal guidance for the acceptance of naked ballots and ignored direction from the Pennsylvania Supreme Court to fix the matter. She allowed ballots to be illegally cured in contravention of state law and pushed the legal envelope for accepting ballots after Election Day.

In the Keystone State, and as with Georgia's Three-card Monte, shuffle fake ballots out from underneath a table scandal, there is also the equally unresolved matter of possible fake ballot manufacturing. Recall, here, the testimony of a truck driver who swears he picked up as many as 100,000 fake manufactured ballots in New York and delivered them to Pennsylvania. Both the tractor-trailer and the ballots involved remain unaccounted for – and what might have been in this tractor-trailer were enough ballots alone to swing the election to Joe Biden.

Finally, in Wisconsin, the mother of all contestable process fouls is arguably that of the roughly 170,000 mail-in ballots entering the tabulation process under the guise of absentee ballots in clear violation of state law. That's more than eight times the number of ballots of the alleged Biden victory margin of 20,682 votes.

In Wisconsin, there is likewise the large-scale abuse associated with an overly expansive definition of "indefinitely confined voters." Recall here that the increment of new indefinitely confined voters in the 2020 election in Wisconsin was more than five times the alleged Biden victory margin.

****

While Democrat Party government officials cheated and gamed the electoral process across all six battleground states, many Republican government officials – from governors and state legislators to judges – did little or nothing to stand in their way.

Consider that the Republican Party controls *both* chambers of the State Legislatures in five of the six battleground states – Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin.[145] These State Legislatures clearly have both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so – and thereby failed both their states and this nation as well as their party.

The same can be said for the Republican governors in two of the six battleground states – Arizona and Georgia. Both Arizona's Doug Ducey and Georgia's Brian Kemp have cowered in their Governor's mansions and effectively sat on their hands while their states have wallowed in election irregularities.

The judicial branch of the American government should be the final backstop for the kind of issues examined in this report. Yet both our State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to properly adjudicate the election irregularities that have come before them. Their failures likewise pose a great risk to the American Republic.

Concluding Observations

From the findings of this report, it is possible to infer what may well have been a coordinated strategy to effectively stack the election deck against the Trump-Pence ticket. Indeed, the patterns of election irregularities observed in this report are so consistent across the six battleground states that they suggest a coordinated strategy to, if not steal the election, then to strategically game the election process in such a way as to unfairly tilt the playing field in favor of the Biden-Harris ticket.

A major part of this "stuff the ballot box" strategy has been aptly summarized in a complaint filed before the US Supreme Court by the State of Texas:

> *Using the COVID-19 pandemic as a justification, [Democrat] government officials [in Georgia, Michigan, Pennsylvania, and Wisconsin] usurped their legislatures' authority and unconstitutionally revised their state's election statutes. They accomplished these statutory revisions through executive fiat or friendly lawsuits, thereby weakening ballot integrity.*[146]

According to the Texas complaint – which the Supreme Court sadly refused to hear – the goal of this strategy was to flood the battleground states "with millions of ballots to be sent through the mails, or placed in drop boxes, with little or no chain of custody." At the same time, Democrat government officials also sought to "weaken the strongest security measures protecting the integrity of the vote signature verification and witness requirements."[147]

The findings of the assessment conducted in this report are consistent with the Texas complaint. Key takeaways include:

- The weight of evidence and patterns of irregularities uncovered in this report are such that it is irresponsible for anyone – especially the mainstream media – to claim that there is "no evidence" of fraud or irregularities.

- The ballots that have come into question because of the identified election irregularities are more than sufficient to swing the outcome in favor of President Trump should even a relatively small portion of these ballots be ruled illegal.

- While all six battleground states exhibit most, or all, six dimensions of election irregularities, each state has a unique mix of issues that might be considered "most important." To put this another way, all battleground states are characterized by the same or similar election irregularities; but, like Tolstoy's unhappy families, each battleground state is different in its own election irregularity way.

- This was theft by a thousand cuts across six dimensions and six battleground states rather than any one single "silver bullet" election irregularity.

- In refusing to investigate a growing number of legitimate grievances, the anti-Trump media and censoring social media are complicit in shielding the American public from the truth. This is a dangerous game that simultaneously undermines the credibility of the media and the stability of our political system and Republic.

- Those journalists, pundits, and political leaders now participating in what has become a Biden Whitewash should acknowledge the six dimensions of election irregularities and conduct the appropriate investigations to determine the truth about the 2020 election. If this is not done before Inauguration Day, we risk putting into power an illegitimate and illegal president lacking the support of a large segment of the American people.

- The failure to aggressively and fully investigate the six dimensions of election irregularities assessed in this report is a signal failure not just of our anti-Trump mainstream media and censoring social media but also of both our legislative and judicial branches.

    - Republican governors in Arizona and Georgia together with Republican majorities in both chambers of the State Legislatures of five of the six battleground states – Arizona, Georgia, Michigan, Pennsylvania, and Wisconsin[148] – have had both the power and the opportunity to investigate the six dimensions of election irregularities presented in this report. Yet, wilting under intense political pressure, these politicians have failed in their Constitutional duties and responsibilities to do so – and thereby failed both their states and this nation as well as their party.

    - Both State courts and Federal courts, including the Supreme Court, have failed the American people in refusing to appropriately adjudicate the election irregularities that have come before them. Their failures pose a great risk to the American Republic.

- If these election irregularities are not fully investigated prior to Inauguration Day and thereby effectively allowed to stand, this nation runs the very real risk of never being able to have a fair presidential election again – with the down-ballot Senate races scheduled for January 5 in Georgia an initial test case of this looming risk.

ENDNOTES

[1] All witnesses who have signed sworn affidavits or declarations who are referenced in this report but whose names are not referenced in the public record, e.g., a court case, are referred to as "Jane Doe" or "John Doe" based on gender. This has been done to ensure their safety and security.

[2] Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan_composition_of_state_legislatures

[3] Bump, Philip. "The two states that almost always predict which candidate is headed for defeat," *The Washington Post*, 7 September 2016. https://www.washingtonpost.com/news/the-fix/wp/2016/09/07/the-two-states-that-almost-always-predict-which-candidate-is-headed-for-defeat/

*The two Democrat candidate exceptions were John F. Kennedy in 1960 and Bill Clinton in 1992.

[4] Williams, Pete. "Trump's election fight includes over 50 lawsuits. It's not going well." *NBC News*, November 23, 2020. https://www.nbcnews.com/politics/2020-election/trump-s-election-fight-includes-over-30-lawsuits-it-s-n1248289

[5] All witnesses who have signed sworn affidavits and declarations referenced in this report are referred to as "Jane Doe" and "John Doe" based on gender, in order to ensure their safety and security.

[6] Bannon, Steve, *War Room Pandemic*, https://pandemic.warroom.org/

[7] Solomon, John, *Just the News*, https://justthenews.com/john-solomon

[8] Kassam, Raheem, *National Pulse*, https://americasvoice.news/the-national-pulse/

[9] *Newsmax*, https://www.newsmax.com/

[10] *One America News Network*, https://www.oann.com/

[11]"Most Say Mail-In Voting Worked, But 47% Say Fraud Likely." *Rasmussen Reports*, December 7, 2020. https://www.rasmussenreports.com/public_content/politics/elections/election_2020/most_say_mail_in_voting_worked_but_47_say_fraud_likely

[12] Legal Information Institute, "Bribery," *Cornell University*, https://www.law.cornell.edu/wex/bribery

[13] Bedard, Paul, "Pro-Biden effort offered Native Americans $25-$500 Visa gift cards and jewelry to vote," *Washington Examiner*, December 14, 2020. https://www.washingtonexaminer.com/washington-secrets/pro-biden-effort-offered-native-americans-25-500-visa-gift-cards-jewelry-to-vote

[14] Pentochoukov, Ivan, "Illegal Money-for-Votes Raffles Conducted in Several States in 2020 Election," *Epoch Times*, December 2, 2020. https://www.theepochtimes.com/illegal-money-for-votes-raffles-conducted-in-several-states-in-2020-election_3598915.html

[15] Morgan, Jessy. Testimony. "A truck driver with USPS says he was suspicious of his cargo load of 288,000 completed ballots." December 1, 2020. https://www.youtube.com/watch?v=R0xaA4dYsbQ

[16] Declaration of John Doe, Delaware County Pennsylvania, November 9, 2020.

[17] Bedard, Paul, "20 House Republicans demand Barr investigate 'suitcases' of ballots in Georgia," *The Washington Examiner*, December 4, 2020. https://www.washingtonexaminer.com/washington-secrets/20-house-gop-demand-ag-barr-investigate-suitcases-of-ballots-in-georgia

[18] "Trump Campaign lawyers present video 'evidence' of ballot fraud," *Senate Judiciary Subcommittee*, December 4, 2020. https://www.youtube.com/watch?v=LJ0xDWhWUxk

Real American Politics, December 4, 2020. https://twitter.com/RealAPolitics/status/1334754269052997635?s=20

[19]See, for example: Weber, Peter, "Georgia's top election investigator debunks a vote fraud conspiracy involving 'suitcases' of ballots, a urinal," December 7, 2020. https://news.yahoo.com/georgias-top-election-investigator-debunks-115236191.html

[20] In the United States District Court for the District of Arizona, *Tyler Bowyer et al v.. Doug Ducey*, December 2, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Bower-Complaint-AZ.pdf

[21] Affidavit of Jane Doe, Cobb County, Georgia, November 12, 2020.

[22] Declaration of Jane Doe, Bucks County, Pennsylvania, Nov 7, 2020

[23] *WisGOP*, "WisGOP: Trump lawsuit highlights indefinitely confined voter increase," https://www.wispolitics.com/2020/wisgop-trump-lawsuit-highlights-indefinitely-confined-voter-increase/

[24] *WisGOP*, "WisGOP: Some indefinitely confined voters are not indefinitely confined," https://www.wispolitics.com/2020/wisgop-some-indefinitely-confined-voters-are-not-indefinitely-confined/

[25] *WisGOP*, "WisGOP: Some indefinitely confined voters are not indefinitely confined," https://www.wispolitics.com/2020/wisgop-some-indefinitely-confined-voters-are-not-indefinitely-confined/

[26] *WisGOP*, "WisGOP: Trump lawsuit highlights indefinitely confined voter increase," https://www.wispolitics.com/2020/wisgop-trump-lawsuit-highlights-indefinitely-confined-voter-increase/
[27] Legal Information Institute, "18 U.S. Code § 611.Voting by aliens," https://www.law.cornell.edu/uscode/text/18/611
[28] The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger,* December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf
[29] In the Superior Court of Fulton County State of Georgia, November 30, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/2020-11-30-Verified-Complaint.pdf
[30] Declaration of Jane Doe, Philadelphia County, Pennsylvania, November 8, 2020.
[31] In the First Judicial District Court Carson City, Nevada *Jesse Law v. Judith Whitmer*, November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf
[32] Declaration of John Doe, Las Vegas, Nevada, November 22, 2020.
[33] "Rudy Giuliani claims 8,000 dead people voted in election in Pennsylvania," November 25, 2020. https://www.youtube.com/watch?v=2_VUkB2jAcg
See Also
"Pennsylvania Senate Republican Lawmaker Hearing Transcript on 2020 Election," *Rev*, November 26, 2020. https://www.rev.com/blog/transcripts/pennsylvania-senate-republican-lawmaker-hearing-transcript-on-2020-election
[34] Affidavit of Jane Doe, Oakland County, Michigan, November 11, 2020.
[35] Declaration of John Doe, Clark County, Nevada, November 7, 2020.
[36] In the Superior Court of Fulton County State of Georgia, *Paul Andrew Boland v Brad Raffensperger*, November 29, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/2020-11-30-Verified-Complaint.pdf
[37] Statement of John Doe, Las Vegas, Nevada, November 20, 2020.
[38] Declaration of Jane Doe, Wisconsin, November 12, 2020.
[39] Affidavit of Jane Doe, Washtenaw County, Michigan, November 9, 2020.
[40] Declaration of Jane Doe, Northampton County, November 8, 2020.
[41] Declaration of John Doe, Philadelphia County, November 14, 2020.
[42] Declaration of Jane Doe, Northhampton County, Pennsylvania, November 7, 2020.
[43] Affidavit of John Doe, Michigan, November 10, 2020.
[44] Declaration of Jane Doe, Clark County, November 8, 2020.
[45] *Ballotopedia*, "How do election workers match signatures? (2020)," https://ballotpedia.org/How_do_election_workers_match_signatures%3F_(2020)
[46]Democratic Party of Georgia, Inc. ("DPG"), the DSCC, and the DCCC, Compromise Settlement and Release, March 6, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/07/GA-Settlement-1.pdf
[47]Petition for Writ of Madamus and Complaint for Declaratory and Injunctive Relief, "*Daniel Rodimer v. Joseph Gloria,* November 19, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/Rodimer-v-Gloria_A-20-825130-W_Writ-of-Mandamus.pdf
[48] In the First Judicial District Court Carson City, Nevada *Jesse Law v. Judith Whitmer*, November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf
[49] In the United States District Court Eastern District of Wisconsin Milwaukee Division, *Donald J. Trump v. the Wisconsin Elections Commission*, December 2, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v-WEC-EDWI.pdf
[50] *Ballotopedia,* "Pennsylvania Secretary of State," https://ballotpedia.org/Pennsylvania_Secretary_of_State
[51] The United States District Court for the Middle District of Pennsylvania, *Donald J. Trump for President et al v. Kathy Boockvar et al,* November, 18 2020. https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf
[52] The United States District Court for the Middle District of Pennsylvania, *Donald J. Trump for President et al v. Kathy Boockvar et al,* November, 18 2020. https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf
[53] The Elections Assistance Commission, "Ballot Building," https://www.eac.gov/sites/default/files/eac_assets/1/6/Chapter_5_Ballot_Building.pdf
[54] Harris, Bev, "About Chain of Custody," *Election Watch*, February 16, 2016. https://blackboxvoting.org/about-chain-of-custody/
[55] Declaration of Jane Doe, Pennsylvania, November 7, 2020. Northhampton County.
[56] Declaration of John Doe, Delaware County, Pennsylvania, November 7, 2020. (3 Pictures, 2 Videos)

[57] In the Supreme Court of the United States, *The State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin*, December 7, 2020. https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/SCOTUSFiling.pdf

[58] Chaitin, Daniel, "Lindsey Graham: Possible ballot harvesting in Pennsylvania involving 25,000 nursing home residents," *Microsoft News,* November 10, 2020. https://www.msn.com/en-us/news/politics/lindsey-graham-possible-ballot-harvesting-in-pennsylvania-involving-25-000-nursing-home-residents/ar-BB1aR3R4

[59] Affidavit of Jane Doe, Brookfield, Wisconsin, November 10, 2020.

[60] Declaration of John Doe, Brown County, November 11, 2020.

[61] Greenberg, Jay, "Dominion Technician Exposed as Anti-Trump Ex-Kamala Harris Worker," December 1, 2020. https://neonnettle.com/news/13425-dominion-technician-exposed-as-anti-trump-ex-kamala-harris-worker

[62] Declaration of Jane Doe, Waukesha County, Wisconsin, November 11, 2020.

[63] " 'USPS contractor: "Something profoundly wrong occurred in Wisconsin during the presidential election' " December 1, 2020. https://www.youtube.com/watch?v=hRUvP6cbtZk&feature=youtu.be&t=69

See also

Van Brugen, Isabel, "Wisconsin USPS Subcontractor Alleges Backdating of Tens of Thousands of Mail-In Ballots," December 2, 2020. https://www.theepochtimes.com/wisconsin-usps-subcontractor-alleges-backdating-of-tens-of-thousands-of-mail-in-ballots_3601580.html

[64] State of Michigan Judicial District, *Cheryl A. Constantino and David A. Kallman v. City of Detroit,* November 8, 2020. https://assets.documentcloud.org/documents/20403147/wayne-county-michigan-election-fraud-lawsuit.pdf

[65] Affidavit of Jane Doe, Oakland County, Michigan November 10, 2020.

[66] Declaration of John Doe, Cobb County, Georgia, November 5, 2020.

[67] Affidavit John Doe, Eagle County, Colorado November 12, 2020.

[68] The Declaration of John McBlain, Esquire. *See*, The Supreme Court of the United States, *State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin,* December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/22O155/163048/20201208132827887_TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf

[69] Affidavit of Jane Doe, Gwinnett County, Georgia, November 12, 2020.

[70] Affidavit John Doe, Waukesha County, Wisconsin, November 10, 2020.

[71] Affidavit of Jane Doe, Clark County, Nevada, November 10, 2020.

[72]The Declaration of John McBlain, Esquire. *See*, The Supreme Court of the United States, *State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin,* December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/22O155/163048/20201208132827887_TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf

[73] Affidavit of John Doe, November 10, 2020, Waukesha County, Wisconsin.

[74] The Declaration of John McBlain, Esquire. *See*, The Supreme Court of the United States, *State of Texas v. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin,* December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/22O155/163048/20201208132827887_TX-v-State-ExpedMot%202020-12-07%20FINAL.pdf

[75] The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger,* December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf

[76] Liptak, Adam, "Supreme Court Allows Longer Deadline for Absentee Ballots in Pennsylvania and North Carolina," *New York Times*, October 28, 2020. https://www.nytimes.com/2020/10/28/us/supreme-court-pennsylvania-north-carolina-absentee-ballots.html

[77] Southwick, Ron, "Pa. received 10,000 ballots after polls closed on Election Day," *PennLive,* Nov10, 2020. https://www.pennlive.com/elections/2020/11/pa-received-10000-late-ballots-that-arrived-after-polls-closed-on-election-day.html

[78] Declaration of Jane Doe, Delaware County, Pennsylvania, November 7, 2020.

[79] The Supreme Court of Wisconsin, "Donald J. Trump et al v. Anthony Evers et al" December 1, 2020. https://cdn.donaldjtrump.com/public-files/press_assets/wisconsin-filing-12-1-20_compressed.pdf

[80] Declaration of Jane Doe, Oak Creek, Wisconsin, November 11, 2020.

[81] The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger,* December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf

[82] Declaration of John Doe, Montgomery County, Pennsylvania, November 7, 2020.

[83] Declaration of John Doe, Allegheny County, Pennsylvania, November 9, 2020.

[84] Declaration of John Doe, Ingham County, Michigan, November 11, 2020.

[85] Declaration of Jane Doe, Ingham County, Michigan, November 11, 2020.

[86] Declaration of Jane Doe, Wheaton, Illinois, November 9, 2020.
[87] "Cure period of absentee and mail-in ballots," *Ballotpedia*, Accessed on December 14, 20. https://ballotpedia.org/Cure_period_for_absentee_and_mail-in_ballots
[88] "Cure period of absentee and mail-in ballots," *Ballotpedia*, Accessed on December 14, 20. https://ballotpedia.org/Cure_period_for_absentee_and_mail-in_ballots
[89] Declaration of Jane Doe, Centre County, Pennsylvania, November 11, 2020.
[90] The United States District Court for the Middle District of Pennsylvania, *Donald J. Trump for President et al v. Kathy Boockvar et al,* November 18, 2020. https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf
[91] The United States District Court for the Middle District of Pennsylvania, *Donald J. Trump for President et al v. Kathy Boockvar et al,* November 18, 2020. https://www.courtlistener.com/recap/gov.uscourts.pamd.127057/gov.uscourts.pamd.127057.169.0.pdf
[92] Declaration of Bartholomew W. and Jean B. W., Milwaukee County, Wisconsin, November 16, 2020. *See Also* https://www.jsonline.com/story/news/2020/11/11/fact-check-republicans-claim-wisconsin-clerks-illegally-altered-ballots/6234023002/
[93] Declaration of John Doe, Delaware County Pennsylvania, November 9, 2020.
[94] State of Michigan Court of Appeals, "*Donald J. Trump for President et. al v. Jocelyn Benson,*" November 30, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/Trump-brief-FINAL.pdf
[95] Affidavit of Jane Doe, Washtenaw County, Michigan, November 9, 2020.
[96] Cornell University, "Equal Protection," *Legal Information Institute*, https://www.law.cornell.edu/wex/equal_protection
[97] Lai, Jonathan et al, " Joe Biden won 3 of every 4 mail ballots in Pennsylvania. Trump won 2 of 3 votes cast in person. What does that mean for the future?" *The Philadelphia Inquirer*, https://www.inquirer.com/politics/election/mail-ballots-pennsylvania-election-trump-biden-20201119.html
[98] Declaration of John Doe, County of Milwaukee, Wisconsin, November 11, 2020
[99] Blair County, Berks County, Lancaster County, Carbon County, Clinton County, Lycoming County, Dauphoin County, and Perry County.
[100] *Joseph D. Hamm v. Kathy Boockvar*, Commonwealth Court of Pennsylvania, November 3, 2020. http://www.pacourts.us/assets/files/setting-7723/file-10362.pdf?cb=f327ff
[101] Secretary of State of Arizona, "Voters have a limited amount of time to correct certain ballot issues," November 9, 2020. https://azsos.gov/about-office/media-center/press-releases/1248
[102] In the United States District Court for the District of Arizona, *Tyler Bowyer et al v.. Doug Ducey*, December 2, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Bower-Complaint-AZ.pdf
[103] *National Conference of State Legislatures*, "Poll Watchers and Challengers," October 1, 2020. https://www.ncsl.org/research/elections-and-campaigns/poll-watcher-qualifications.aspx
[104] *National Conference of State Legislatures*, "Poll Watchers and Challengers," October 1, 2020. https://www.ncsl.org/research/elections-and-campaigns/poll-watcher-qualifications.aspx
[105] Affidavit of Jane Doe, Rockdale County, Georgia, November 2020.
[106] Declaration of John Doe, Philadelphia, Pennsylvania, November 8, 2020.
[107] Affidavit of Jane Doe, Brookfield, Wisconsin, November 10, 2020.
[108] *Ballotopedia*, "Voting Equipment and Methods by State," https://ballotpedia.org/Voting_methods_and_equipment_by_state
[109] *Ballotopedia*, "Voting Equipment and Methods by State," https://ballotpedia.org/Voting_methods_and_equipment_by_state
[110] *Dominion Voting Systems,* "About," https://www.dominionvoting.com/about/
[111] Varnona, Frank "2020 Stolen Election by Dominion Voter Systems – Hammer & Scorecard," Conservative Business Journal, https://www.conservativebusinessjournal.com/2020-stolen-election-hammer-and-scorecard/
[112] *Clinton Foundation*, "The Delian Project," https://www.clintonfoundation.org/clinton-global-initiative/commitments/delian-project-democracy-through-technology
[113] For example, the Chairman of Smartmatic, Mark Malloch-Brown, is on the board of George Soros' Open Society Foundation. *Open Society Foundation*, "Leadership," https://www.opensocietyfoundations.org/who-we-are/leadership/mark-malloch-brown
[114] The First Judicial Court in Carson City, Nevada, "*Jesse Law et al v. Judith Whitmer et al,*" November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf
[115] The First Judicial Court in Carson City, Nevada, "*Jesse Law et al v. Judith Whitmer et al,*" November 17, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/11/nov-17-doc-2.pdf

[116] "In violation of Nevada law, the Clark County Election Department allows the Agilis machine to solely verify 30% of the signatures accompanying the mail-in ballots without ever having humanize inspect those signatures."
[117] In the Superior Court of Arizona in and For the County of Maricopa, "*Kelli Ward v. Constance Jackson et al*," November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf
[118] In the Superior Court of Arizona in and For the County of Maricopa, "*Kelli Ward v. Constance Jackson et al*," November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf
[119] Affidavit of John Doe, Dallas County, Texas. November 17, 2020. https://www.courtlistener.com/recap/gov.uscourts.gand.283580/gov.uscourts.gand.283580.7.1_2.pdf
[120] Ramsland Jr., Russell. "Antrim Michigan Forensics Report." *William Bailey v. Antrim County, Michigan*, December 13, 2020. https://depernolaw.com/uploads/2/7/0/2/27029178/antrim_michigan_forensics_report_[121320]_v2_[redacted].pdf
[121] "Excerpts from the 2002 FEC Voting System Standards – 3.2.1 Accuracy Requirements." *Michigan Secretary of State.* https://www.michigan.gov/sos/0,4670,7-127-1583-130621--,00.html
[122] "Document Retention Schedule." *Michigan Bureau of Elections*, May 2019. https://www.michigan.gov/documents/sos/Document_Retention_Schedule_412493_7.pdf
[123] Sperry, Paul. "Georgia voting irregularities: The curious case of Biden's 20,000-vote surge." *The Citizen*, November 15,2020. https://thecitizen.com/2020/11/15/georgia-voting-irregularities-the-curious-case-of-bidens-20000-vote-surge/
[124] Parks, Miles, "Why Some Mail-In Ballots Are Rejected As Invalid," *NPR*, October 4, 2020. https://www.npr.org/2020/10/04/920175418/why-some-mail-in-ballots-are-rejected-as-invalid
[125] Livingston, Doug, "Why absentee ballots get rejected, and how to make yours count," *USA Today*, September 21, 2020. https://www.beaconjournal.com/story/news/2020/09/21/why-absentee-ballots-rejected-presidential-and-other-elections/3486553001/
[126] Livingston, Doug, "Why absentee ballots get rejected, and how to make yours count," *USA Today*, September 21, 2020. https://www.beaconjournal.com/story/news/2020/09/21/why-absentee-ballots-rejected-presidential-and-other-elections/3486553001/
[127] Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf
[128] *Ballotopedia,* "Election results, 2020: Analysis of rejected ballots," December 11, 2020. https://ballotpedia.org/Election_results,_2020:_Analysis_of_rejected_ballots
See Also
Office of Nevada Secretary of State Barbara K. Cegavske, "2020 General Election Turnout Mail Ballot Information," https://www.nvsos.gov/sos/home/showdocument?id=9058
[129] Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf
[130] *Ballotopedia,* "Election results, 2020: Analysis of rejected ballots," December 11, 2020. https://ballotpedia.org/Election_results,_2020:_Analysis_of_rejected_ballots
See Also
U.S. Elections Project, "Pennsylvania Early Voting Statistics," November 20, 2020. https://electproject.github.io/Early-Vote-2020G/PA.html
[131] Election Assistance Commission, "The Election Administration and Voting Survey; A Report to the United States Congress," 2016. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf
[132] The Superior Court Of Fulton County State Of Georgia, *Trump v. Raffensperger,* December 4, 2020. https://www.democracydocket.com/wp-content/uploads/sites/45/2020/12/Trump-v.-Raffensperger.pdf
[133] For example, in Pennsylvania, 3 out of every 4 absentee/mail-in ballots went to Joe Biden https://www.inquirer.com/politics/election/mail-ballots-pennsylvania-election-trump-biden-20201119.html
And in Milwaukee, Wisconsin, 84% of absentee/mail-in ballots went to Joe Biden
https://www.tmj4.com/news/election-2020/no-joe-biden-did-not-get-100-percent-of-all-milwaukee-absentee-ballots
[134] Heine, Debra,"Mathematician Says Biden May Have Received 130 Percent of the Democrat Vote in Maricopa County, Arizona," December 2, 2020. https://themichiganstar.com/2020/12/02/mathematician-says-biden-may-have-received-130-percent-of-the-democrat-vote-in-maricopa-county-arizona/
[135] Affidavit of Russel R., Dallas County, Texas. November 17, 2020. https://www.courtlistener.com/recap/gov.uscourts.gand.283580/gov.uscourts.gand.283580.7.1_2.pdf

[136] *Milwaukee City Wire News Service*,"Analysis: Five Milwaukee wards report 89% turnout in 2020 presidential vote; Biden nets 146K votes in city," November 4, 2020. https://mkecitywire.com/stories/564495243-analysis-seven-milwaukee-wards-report-more-2020-presidential-votes-than-registered-voters-biden-nets-146k-votes-in-city

[137] *Milwaukee City Wire News Service*,"Analysis: Five Milwaukee wards report 89% turnout in 2020 presidential vote; Biden nets 146K votes in city," November 4, 2020. https://mkecitywire.com/stories/564495243-analysis-seven-milwaukee-wards-report-more-2020-presidential-votes-than-registered-voters-biden-nets-146k-votes-in-city

[138] Duda, Jeremy. "GOP lawsuit questions 'duplicate' ballots in Queen Creek," *San Tan Valley Sentinel*, November 27, 2020. https://www.pinalcentral.com/san_tan_valley_sentinel/local_news/gop-lawsuit-questions-duplicate-ballots-in-queen-creek/article_ee9557d0-97e4-53e9-a269-5beb4b64370a.html

[139] In the Superior Court of Arizona in and For the County of Maricopa, *Kelli Ward v. Constance Jackson et al*, November 24, 2020. https://assets.documentcloud.org/documents/20417265/ward-v-jackson-complaint-and-petition-for-discovery.pdf

[140] *Voter Integrity Project*, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020

[141] *Voter Integrity Project*, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020

[142] *Voter Integrity Project*, "Anomalies in Vote Counts and Their Effects on Election 2020," November 24, 2020. https://votepatternanalysis.substack.com/p/voting-anomalies-2020

[143] *News Now*, "Michigan Republican Electors Harassed And Forced To Change Vote," November 18, 2020. https://www.youtube.com/watch?v=YW1YzQY_1Ro

Dowling, M. "Michigan's largest county refuses to certify the election – Update, evil wins," *Independent Sentinel*, November 17, 2020. https://www.independentsentinel.com/michigans-largest-county-refuses-to-certify-the-election/

See Also

Institute for Political Economy, "Wayne County Michigan Withdraws Election Certification, Security Expert Concludes Michigan Was Stolen." https://www.newsbreak.com/news/2105758771365/wayne-county-michigan-withdraws-election-certification-security-expert-concludes-michigan-was-stolen

[144] Pentchoukov, Ivan, "Illegal Money-For-Votes Raffles Conducted in Several States in 2020 Election," December 1, 2020. https://www.theepochtimes.com/illegal-money-for-votes-raffles-conducted-in-several-states-in-2020-election_3598915.html

[145] Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan_composition_of_state_legislatures

[146] *State of Texas v. The Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin*, "Motion for Leave to File Bill of Complaint," December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/22O155/162953/20201207234611533_TX-v-State-Motion-2020-12-07%20FINAL.pdf pg. 1

[147] *State of Texas v. The Commonwealth of Pennsylvania, State of Georgia, State of Michigan, State of Wisconsin*, "Motion for Leave to File Bill of Complaint," December 7, 2020. https://www.supremecourt.gov/DocketPDF/22/22O155/162953/20201207234611533_TX-v-State-Motion-2020-12-07%20FINAL.pdf pg. 1

[148]Ballotopedia, "Partisan composition of state legislatures," December 4, 2020. https://ballotpedia.org/Partisan_composition_of_state_legislatures