THE FOLLOWING ESTABLISHES "FOREIGN INTERFERENCE" IN THE UNITED STATES 2020 ELECTIONS AS DEFINED IN E.O. 13848

> *"…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."*
>
> – Definition of "foreign interference" with respect to an election per Executive Order 13848 (2018).

The President of the United States, pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333 and 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code, has already found a national emergency regarding the elections since 2018. The following list is of evidence and findings already made of foreign

interference in the November 2020 General Election—especially by Iran.[1] There is additional evidence developing of foreign interference from China.

On September 12, 2018, through Executive Order 13848, the President declared a national emergency to address the threat of foreign interference in a United States election based on findings that the ability of persons outside the United States to interfere with 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, constituted an unusual and extraordinary threat to the national security and foreign policy of the United States.

The national emergency persists and conditions have dramatically worsened. There is now clear and definitive evidence of both foreign interference and widespread election fraud impacting processes and critical infrastructure before, during and after the US General Election of November 3, 2020. Additional evidence of foreign election interference surfaces daily.

As the FBI and CISA (Cybersecurity and Infrastructure Security Agency) have already found with respect to this election, these unprecedented attacks on critical election infrastructure are designed to undermine the integrity and reliability of

1

American elections, and thereby strike at the heart of this Republic. Such malicious activity is destabilizing and detrimental to the national security, economic security, and foreign policy of the United States. Urgent action is necessary to secure and preserve U.S. election systems, and additional forensic assessment should be conducted immediately to determine the full extent of foreign interference and unauthorized access to critical election infrastructure.

These challenges we now face as a nation have been compounded by censorship and disinformation campaigns of foreign and domestic adversaries, in combination with social media companies, "news" outlets, and search engines. Collectively, these entities have engaged in systematic censorship of information – specifically, evidence of foreign interference and widespread fraud and criminal activity in the 2020 General Election, while actively spreading misinformation about these matters of national importance, thereby facilitating the destabilization of the American political process.

A sampling of evidence and information concerning foreign election interference and related matters is therefore included below for the public benefit. The evidence shows:

a) **There was foreign interference in the November 3, 2020 election.** Foreign interference was observed and documented by experts and data analysts, including the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA). Multiple expert witnesses and cyber experts identified acts of foreign interference in the

election in the days immediately prior to November 3, 2020 and continuing in the following weeks.

b) **Election machines and software used by most voters across the country are compromised.** The five companies which provide systems that control voting in the United States are Dominion, ES & S, Hart InterCivic, Sequoia, and Smartmatic. The three largest vendors – Dominion, ES & S, and Hart InterCivic – collectively provide machines and software for over 90% of all eligible U.S. voters. The numerous similarities between these voting systems are related to shared origin of the software code, and all of the systems have similar security and functional flaws.

c) **Individuals and firms that are foreign (or which have substantial foreign ties) own or control each of these vendors.** Additionally, approximately 20% of the components used in these voting machines are from China-based companies. In addition, there is currently evidence of direct interference from China in the Georgia run-off elections.

d) **These election systems appear to have been intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results.**

The President is the Chief Law Enforcement Officer and Commander in Chief of the United States of America. It is the duty of the President to protect and defend the Constitution and laws of the United States. This requires taking action to protect

national security and the country's critical infrastructure, including the security and integrity of our voting systems necessitated by foreign interference in the November 3, 2020 elections.

Consistent with these facts findings, and his sworn duty as President, the President should invoke all authorities to act to protect the Republic of the United States of America, the country's critical election and cyber infrastructure, election integrity, and all related national interests, and pursuant to Executive Order 13848, immediately take all legal action appropriate and within the power of the President to determine the true legal votes and outcome of this election.

***

HIGHLIGHTS OF THE EVIDENCE

1) **The Bipartisan Report of the Senate Intelligence Committee issued on August 18, 2020 warned of the known vulnerabilities of major voting systems used throughout the country and the likelihood of fraud and hacking in the upcoming elections.**
   - **a)** According to the report, beginning by at least 2014, "the Russian government directed extensive activity against the U.S. election infrastructure," but there was "no evidence any votes were changed or voting machines manipulated."
   - **b)** The Department of Homeland Security designated the "election infrastructure" of the United States as a "Critical Infrastructure Subsector." See SSCI Report: 3 and n. 1 (2018).

c) By the end of 2018, "the Russian cyber actors had successfully penetrated Illinois' voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records." SSCI Report: 22 (2018).

d) In 2018, "Congress appropriated $380 million in grant money for the states to bolster cybersecurity and replace vulnerable voting machines." SSCI Report: 5

e) The SSCI found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in the elections.

f) GEMS Software is common to each of these voting systems. GEMS has been owned by Dominion since 2010, when an antitrust suit brought by then-Attorney General Eric Holder ended with the divestiture of Diebold's Premier division and its acquisition by Dominion was approved by the Department of Justice.

g) "ES & S Voting Systems disclosed that some of its equipment had key security vulnerability. ES & S installed remote access software on machines it sold in the mid-2000s, which . . . created potential remote access into the machines." SSCI Report: 41. Three hundred voting jurisdictions used the software, and 41 states used it products. Id.

h) The Committee heard disturbing testimony of the ability of operators to "reprogram the machine to invisibly cause any candidate to win." Id. At 42. It is undisputed that the FBI and the National Security Division of the DOJ knew of these national security issues and threats. Id. At 43.

i) The Committee identified problems with vendors, supply chains, the absence of any regulatory authority requiring vendors to adhere to basic security practices. **"If there is no way to audit the election, that is absolutely a national security concern**." Minority Views of Senator Wyden, Report: 2 (2018). Notably, Dominion Voting Systems do not maintain a truly auditable trail for a number of reasons, among them being that its audit logs are editable by operators (and by those with unauthorized access).

j) Dominion is used in 22 states and 600 local jurisdictions. For example, in the Summer 2019, the State of Georgia purchased Dominion Voting Systems for its operations state-wide at a contract price of $107 million.

2) **Dominion Voting Systems and Scytl/Clarity Elections:**

a) Dominion Voting Systems is owned and controlled by foreign entities. As a National Security concern, having foreign entities managing US elections gives foreign actors strategic but hidden influence upon the future of foreign policy, National Security Strategy, and National Military Strategy. Since these companies move data around the world, malign foreign states, and actors – or even opportunistic foreign states and actors – have ability to influence (or even determine) election outcomes in ways that are most favorable to their government or causes. This impacts all the elements of US National Security; Diplomacy; Information; Military; Economic; Financial; Intelligence; and Law Enforcement (DIMEFIL).

b) It is a fact that the US institutions listed above are under constant cyber-attack. Attacking the election system to control the administration taking power of the largest economy in the world is a singular assault on all of the DIMEFIL pillars of national power at once.

c) Electronic data from US elections was transmitted to Germany, Barcelona, Serbia, and Canada.

   i) **Dominion Servers** in Belgrade Serbia. P 82.117.198.54 (ASN Range: 82.117.192.0/19)

   ii) **Dominion Servers** ftp.dominionvoting.com with IP 69.172.237.100 (ASN Range: 69.172.236.0/22) is located in Toronto, Canada

   iii) The website www.scytl.com with IP 52.57.209.147 (ASN Range: 52.57.0.0/16) is (was) located in **Frankfurt Germany.**

   iv) The website support.scytl.com with IP 213.27.248.118 (ASN Range: 213.27.128.0/17) is located in **Barcelona, Spain**

   v) The website scytl-com.mail.protection.outlook.com with IP 104.47.10.36 (ASN Range: 104.40.0.0/13) is located in **Ireland.**

d) Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests.

e) The forensic report prepared for Antrim County, Michigan found that, "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results".

i) For example, the report found that the system intentionally generates an enormously high number of ballot errors. The intentional errors lead to individual or bulk adjudication of ballots with no oversight, no transparency, and no audit trail.

ii) Dominion operating system has control functions to allow for transfer of adjudication files from one Results Tally system to another. This is the exact type of issue that leads to voter and/or election fraud.

iii) The report found the election management system to be wrought with unacceptable vulnerabilities—including access to the internet— a key indicator to find evidence of fraud, and numerous malicious actions.

f) On election night the DE-CIX Frankfurt ("The World's Leading Internet Exchange") experienced a significant spike over its previous high traffic peaks. One expert attributed the likely cause to increased data flow to servers supporting the US Election. On November 4, 2020, the firm wrote, "Last night, for the first time, we reached 10 Terabits per second peak traffic at DE-CIX Frankfurt." (cf. https://www.de-cix.net/en/about-de-cix/news/de-cix-frankfurt-hits-10-tbps-peak-traffic)

3) **The numerous similarities among these voting systems are related to common software code.**

a) Further forensic investigation will confirm that Dominion Voting Systems, Smartmatic, Electronic Systems & Software, and Hart Inter Civic, all have

similar security and functional flaws. Clarity Election Night Reporting, Edison Research, Scytl have serious vulnerabilities that were subject to foreign interference in the 2020 election in the United States.

b) These systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in the 2020 US General Election, in which votes were in fact altered and manipulated contrary to the will of the voters, as evidenced by the forensic analysis of Antrim County MI as well as statements of citizens there who witnessed machine alteration of election results.

c) Each of the companies use EML (Election Markup Language) and are susceptible to cross site scripting attacks (XSS) as described on page 7 in the Joint Cybersecurity Advisory. Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

d) Most, if not all, related sites were created using WordPress. WordPress currently has 2,675 CVE (Common Vulnerabilities and Exposures) listed on cve.mitre.org.

e) Experts performed an OpenVAS Vulnerability assessment for both Dominion and Scytl. There were multiple issues related to out-of-date plugins and themes, which leaves sites vulnerable to attack.

f) Dominion's purchase of Sequoia Voting Systems from Smartmatic has resulted in the same **"Source Code"** being used today. Due to this and various other mergers, acquisitions, licensing agreements and partnerships, the entire election ecosystem in the United States is convoluted, murky and hidden. This began with the Venezuelan investment into Smartmatic specifically to rig elections. It should also be noted that Smartmatic still runs elections in the US and licenses its software to other Election Management System Companies.

g) The refusal to inspect software code goes against common US legal and business practice. It is common legal procedure to inspect code under a protective order to determine intellectual property suits. The claims from all of these companies that their code should not be inspected is a strong indicator of malign activity.

h) During a recent forensic audit, experts discovered WinEDs and GEMS in the Dominion Voting System EMS (Election Management System). Both of those

modules have been included in adverse findings from the EAC but are still in use today.

i) Dominion and Smartmatic share a physical address in Barbados despite their insistence that there is no relationship between the companies. They also have a mutual non- compete agreement detailing shared resources and code.

j) The fact that a Smartmatic board member, Peter Neffenberger, is named as a key member of the presidential transition team is a significant conflict of interest. Additionally, members of George Soros' Open Society Foundations are also serving board members of Smartmatic.

k) Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software and trademarks to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom.

l) Given the overlap between Dominion and Smartmatic, including the shared business address in Barbados, the FCC Report ID: 2AGVK-VIU811 issued by the CCIS Lab in Shenzhen, China is very concerning. The **Voter Identification Unit** report was issued on July 23, 2020 and would give China insight on how to exploit the voting machines used in the US Election.

4) **Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks.**

a) There is evidence of a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017). This is compounded by the magnitude of the Solar Winds exploit that has exposed the private, public and government related companies and agencies. This includes the companies and agencies directly involved with securing our elections.

b) The FBI and CISA issued a joint Cybersecurity Advisory on October 30, 2020 (Report ID: AA20-304A). 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.

5) **Staple Street Partners**

a) Staple Street Partners is an equity firm that owns Dominion Voting Systems.

b) Hootan Yaghoobzadeh is the CEO and Chairman of Staple Street Capital, which is the entity that owns Dominion. Yaghoobzadeh was a close confidant to Sadaam Hussein and worked for the Saudi Bin Laden group. He previously worked at the Carlyle Group and Cerberus Capital Management.

c) Dominion Voting Systems based in Toronto entered into a Security Agreement with HSBC Bank on September 25, 2019, assigning all intellectual property and assets including Trademarks, Patents and Software (see below).

d) On October 8, 2020, $400,000,000 from UBS Securities a Chinese managed subsidiary of UBS Global AG was invested in Dominion Voting Systems.

6) **Since at least 2006, members of Both Parties have complained of defective voting system, especially Dominion Voting Systems.**

a) On October 6, 2006, citing concerns about foreign influence and control over Dominion machines and Smartmatic/Sequoia software, Representative Carolyn B. Maloney sent a letter to the then-Secretary of the Treasury, Henry M. Paulson, Jr. "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." Rep. Maloney explained her view that "this issue demands the most thorough independent investigation by CFIUS" in light of

"publicly reported information about Smartmatic's ownership and about the vulnerability of electronic voting machines to tampering." She states, "[i]t 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.… 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."

b) On December 6, 2019, Senators Elizabeth Warren, Ron Wyden and Amy Klobuchar, and Representative Mark Pocan sent letters to Michael McCarthy of McCarthy Group, LLC that "trouble-plagued companies 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" (internal quotations omitted). The Senators and Congressman articulated concerns about the "highly concentrated" election technology industry, "with a handful of consolidated vendors controlling the vast majority of the market." They explained, "[t]oday, three large vendors – ES&S, Dominon 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." Citing outdated machines and software that is vulnerable to hackers, they noted that "[e]lection security experts have noted for years that our nation's election systems and infrastructure are under

serious threat." Finally, before asking a series of questions, the Senators and Representative detailed a sampling of problems identified during the 2018 election, including specifically that, "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" (internal citations omitted). "In addition," they say, "researchers recently uncovered previously undisclosed vulnerabilities in 'nearly a dozen backend election systems in 10 states.'" They also cite a 2019 incident in Pennsylvania involving a state judicial election, where "the Democratic candidate's electronic tally showed that he received an improbable 164 votes out of 55,000 cast" and the county's Republican Chairwoman acknowledged that "everything went wrong" on Election Day. "These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack," they added.

c) Also on December 6, 2019, Senators Elizabeth Warren, Ron Wyden and Amy Klobuchar, and Representative Mark Pocan sent a similar letter, to Stephen D. Owens and Hootan Yaghoobzadeh of Staple Street Capital Group, LLC based on reports that "Staple Street owns or has had investments in Dominion".

7) **Multiple foreign actors have interfered in voting process of American citizens and the elections held by the United States in October and November 2020.**

a) On October 30, 2020, the FBI and the Department of Homeland Security issued a determination and advisory that **Iran** and **Russia** had obtained and apparently used email addresses from state voter registration lists, which include party affiliation and home addresses and can include phone numbers.

i) It appears that those addresses were then used in a widespread targeted spamming operation. The senders claimed they would know which candidate the recipient was voting for in the Nov. 3 election, for which early voting was ongoing at the time this violation was discovered and notice was issued. Federal officials have long warned about the possibility of this type of operation, as such registration lists are not difficult to obtain.

ii) On October 20, 2020, Christopher Krebs, then the top election security official at the Department of Homeland Security, had tweeted, "These emails are meant to intimidate and undermine American voters' confidence in our elections." This comment clearly falls within the definition of "foreign interference" under E.O. 13848 of September 12, 2018 as, "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".

b) On October 22, 2020, CISA and the FBI issued Alert AA20-296B warning, "Iranian actors are likely intent on influencing and interfering with the US elections to sow discord among voters and undermine public confidence in the US electoral process." The alert further stated that Iranian actors are, "creating fictitious media sites and spoofing legitimate media sites to spread obtained US voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud."

c) On October 30, 2020, CISA and the FBI issued joint Alert (AA20-304A) *Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data* stating that "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". In addition, they wrote, "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. (See FBI FLASH message ME-000138-TT, disseminated October 29, 2020).

   i) 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."** (emphasis added).

ii) This finding of CISA and the FBI of this "intentional effort to influence and interfere with the 2020 U.S. presidential election" by an Iranian advanced persistent threat actor constitutes foreign interference, as defined by E.O. 13848.

d) During the time of election night and the following morning, hundreds of thousands of fraudulent votes entered the U.S. Election system. They did so in amounts, times, and sequences that mathematical and statistical experts have attested are a mathematical impossibility.

8) **Just three weeks prior to the election of November 3, 2020, federal Judge Amy Totenberg found Dominion Voting Systems full of risks by "stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection."**

a) Judge Totenberg heard three days of testimony, including from Dominion executive Eric Coomer. The judge wrote that there are, "true risks posed by the new BMD [Ballot Marking Device of Georgia's Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances."

b) Continuing, she noted "the insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise." The voter does not see his actual ballot. "The printed ballot is fed

into an ImageCast optical scanner that tabulates the ballot votes solely based on the QR code – and not based on the human readable text on the printed ballot."

c) Judge Totenberg was very concerned. She stated: "The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems' capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process."

d) Further, Judge Totenberg wrote: "The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of 'might this actually ever happen?' – but 'when it will happen,' especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, 'we have never seen it,' the future does not bode well. Still, this is year one for Georgia in implementation of this new BMD system as the first state

in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State's doorstep. The Court certainly hopes not."[2]

9) Every defect and hazard of which Judge Totenberg warned happened in Georgia and across the country.

a) Witnesses in Georgia, Arizona, Michigan, Wisconsin, Pennsylvania, and other states, have attested to election computer crashes, replacements of a server, impermissible and untested updates to the system, and connections to the internet—among countless other election law violations and irregularities.

b) Both Coffee and Ware counties in Georgia have identified a significant percentage of votes being wrongly allocated, contrary to the will of the voter. Ware County, Georgia, upon a full hand recount of its ballots, found a 37 vote discrepancy between the electronic tabulation of the vote and the hand recount, identifying a vote flip of 37 votes from President Trump to Biden. Extrapolated over the counties of Georgia corresponds to a more than 56,000 vote difference.

c) Coffee County, Georgia Board of Elections had to refuse to certify its vote because during the November 30, 2020 recount, the Dominion Voting Systems produced 39 new votes for President Trump without any change in total ballots cast. In this same recount, the Board scanned 185 missing recount ballots into

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

the results, yet the Dominion tabulator found no change in the votes for any candidate. On December 2, 2020, during Georgia's third recount, the same original results were produced, ignoring the 185 new ballots.

d) Analysis has established that there was a 5.6 % increase in votes for one candidate for president across the entire Dominion system—with all other variables frozen.