EXHIBIT 9

CONGRESSIONAL TASK FORCE ON

ELECTION SECURITY

FINAL REPORT

January 2018

CONGRESSIONAL TASK FORCE ON ELECTION SECURITY

CO-CHAIR BENNIE G. THOMPSON
MISSISSIPPI

CO-CHAIR ROBERT BRADY
PENNSYLVANIA

REP. ZOE LOFGREN
CALIFORNIA

REP. JAMES R. LANGEVIN
RHODE ISLAND

REP. CEDRIC L. RICHMOND
LOUISIANA

REP. VAL DEMINGS
FLORIDA

Special thanks to staff who contributed to this final report:

Arlet Abrahamian, Collen Altstock, Moira Bergin, Rosaline Cohen, Adam Comis, Jamie Fleet, Hope Goins, Imani Gunn, Zj Hull, Peter Hunter, Nick Leiserson, Brittany Lynch, Kerry Mckittrick, Alison Northrop, Elise Phillips, Tanya Sehgal, Alicia Smith, Nicole Tisdale, Chris Wilcox, and the Democratic Staff of the House Committees on Homeland Security and Administration.

TABLE OF CONTENTS

INTRODUCTION

The Russian interference in the 2016 presidential election called for swift and robust action by the United States government. While the Obama Administration acted with great urgency and determination to assess and address the Russian attacks on the 2016 U.S. election, the Trump Administration and Republican Members of Congress still refuse – a year later – to pursue the facts and defend our democracy.

As a result, House Democratic Leader Nancy Pelosi, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS), and Committee on House Administration Ranking Member Robert Brady (D-PA) announced the formation of the Congressional Task Force on Election Security (the Task Force). The Task Force, consisting of Rep. Bennie G. Thompson (D-MS), Rep. Robert Brady (D-PA), Rep. Zoe Lofgren (D-CA), Rep. James R. Langevin (D-RI), Rep. Cedric L. Richmond (D-LA), and Rep. Val Demings (D-FL), was established to serve as a forum for Members from the House Administration and House Homeland Security Committees to engage with election stakeholders as well as cybersecurity and election infrastructure experts to ensure the health and security of our nation's election systems.

The six Members of Congress worked together over a period of six months with the mission to help maintain free, fair, and secure elections and prevent future damage to our democracy. Over the past six months, the Task Force met with over twenty experts and stakeholders and held two public forums featuring state election officials and former national security officials. Members identified policy recommendations to fortify our election systems, guard against future attacks, and restore voter confidence in our democratic institutions.

EXECUTIVE SUMMARY

In November 2016, 139 million Americans cast their votes in the wake of a massive Russian cyber-enabled influence operation designed to undermine faith in American democracy. The Kremlin spread misinformation and disinformation to the American electorate through more than 1,000 YouTube videos, 130,000 tweets, and 80,000 Facebook posts. The latter were viewed by approximately 126 million people on Facebook platforms alone. Russian agents also hacked into U.S. political organizations and selectively exposed sensitive information through third-party intermediaries like WikiLeaks. Finally, Russia targeted voting systems in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.

The unprecedented attack by Russia exposed serious national security vulnerabilities in our election infrastructure.

On January 6, 2017 then-Department of Homeland Security (DHS) Secretary Jeh Johnson designated election infrastructure as a critical infrastructure subsector, citing the importance of the infrastructure to our national interests and the "more sophisticated and dangerous" risks to the systems.[1] The designation came the same day the Office of the Director of National Intelligence (ODNI) released a declassified report, in coordination with the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA), entitled *Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*. The report found that "Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards," and that the Kremlin "will apply lessons learned…to future election influence efforts worldwide, including against US allies and their election processes."[2]

One year following the attacks, we have a better understanding of the threat to our elections. The Russian government directed efforts to target voting systems in 21 states prior to the 2016 election.[3] Although there is no evidence of the attacks altering the vote count, Kremlin hackers were able to breach at least two states' voter registration databases.[4] Russia's appetite for undermining confidence in western democratic institutions – by disenfranchising voters or calling into question the integrity of election administration by altering voter information – is only growing stronger. In fact, during a hearing before the House Permanent Select Committee on Intelligence, then FBI Director James Comey warned that Russia will be back as it may draw from its intrusions that they were successful "because they introduced chaos and division and discord and sowed doubt about the nature of this amazing country of ours and our democratic process."[5] In addition to Russia, China, Iran, and North Korea remain cybersecurity threats, and we should prepare for the emboldening and response of other nation states.

State and local election officials are acutely aware of the threats they are facing, but they lack the necessary funds to safeguard their voting infrastructure.[6] In most states, legislatures are not increasing their election security budgets.[7] In some cases, Governors are actively undermining election security efforts.[8] Moreover, state and local officials have expressed a desire for Congress to step in. The majority of state election officials surveyed by *Politico* in late 2017 indicated that they needed additional funding from the federal government to replace obsolete election systems and technology and to bolster election security.[9] Indeed, the National

Association of Secretaries of State made clear to the Task Force that "[s]tates would clearly benefit from the appropriation of the outstanding balance of federal HAVA [Help America Vote Act] funds to aid them in ensuring that they have sufficient equipment, technical support, and resources to maintain a sound security posture for their computer-based systems."[10]

This issue is simply too important to sit back and watch state governments and the federal government pass responsibility back and forth. In late December, a bipartisan group of Senators introduced the "Secure Elections Act" that would strengthen our elections and provide states with the resources they need. With the 2018 midterm elections rapidly approaching, it is imperative that the House of Representatives also act to secure our elections and protect the integrity of the ballot box. Our investigation has led us to make the following recommendations:

Federal Funds Should Be Provided to Help States Replace Aging, Vulnerable Voting Machines with Paper Ballots

The Brennan Center estimates that the cost to replace paperless direct-recording electronic voting machine (DREs) would be between $130 and $400 million, and Congress could authorize this money right now. The Help America Vote Act (HAVA) authorized $3 billion to meet the statute's requirements, and over $300 million remains to be appropriated.[11] Congress should act immediately to allow states to use this money.

States Should Conduct Risk-Limiting Post-Election Audits

A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct.[12] A statistically sound post-election audit would enable states to determine that the original vote count was substantially accurate.

Federal Funds Should Be Provided to Help States Upgrade and Maintain IT Infrastructure, Including Voter Registration Databases

States need money to replace outdated technology and hire IT support. It is important to note that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials. Congress must establish a mechanism to provide ongoing support to state and local governments.

Election Technology Vendors Must Secure Their Voting Systems

Many states purchase their voting systems from third-party vendors who have little financial incentive to prioritize election security, and are not subject to regulations requiring them to use cybersecurity best practices. Election vendors should be required to inform Election Assistance Commission (EAC) and DHS officials in the event of a cyberattack. In addition, state contracts should require vendors to: 1) secure their systems, and 2) notify state and local officials in the case of a cyber security incident.

The Federal Government Should Develop a National Strategy to Counter Efforts to Undermine Democratic Institutions

We need a strong, consistent rebuke from the White House. Next, we need the President to acknowledge that we need a "9/11-style" Commission to help identify the various ways in which Russia and other potential threat actors are seeking to undermine democracy and develop a plan to confront them.

The Intelligence Community Should Conduct Pre-Election Threat Assessments Well in Advance of Federal Elections

The Intelligence Community should complete and provide to Congress and state and local election officials an assessment of the full scope of threats to election infrastructure 180 days prior to a federal election, together with recommendations provided by DHS and EAC to address them.

DHS Should Maintain the Designation of Election Infrastructure as a Critical Infrastructure Subsector

Defining election systems as critical infrastructure means election infrastructure will, on a more formal and enduring basis, be a priority for DHS cybersecurity services. This is not the time to diminish federal efforts or shut down important lines of dialogue between DHS and election administrators.

Empower Federal Agencies to be Effective Partners in Pushing out Nationwide Security Reforms

Congress must act and give DHS the resources it needs to meet its obligations to state and local election officials, as well as all critical infrastructure owners and operators. Similarly, Congress should fund the EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.

Establish Clear and Effective Channels for Sharing Threat and Intelligence Information with Election Officials

DHS needs a formalized process to provide real-time appropriate threat information to state and local election officials to improve information flow and help prevent intrusions in our election infrastructure.

States Should Prioritize Cybersecurity Training

States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. It costs money for states to produce training materials, and takes staff time to implement statewide training programs. The federal government should provide training support either through the EAC or by provide funding to states to assist with their training programs.

UNDERSTANDING THE THREAT

THE FOUR GREATEST STATE-ACTOR THREATS

Before addressing recommendations, this report will lay out the capabilities of each of the four state actors that may pose the greatest threat. Using examples drawn from each of these states' past cyber activities, this report will also comment briefly on what might motivate each of these four actors to interfere in future U.S. elections

Russia

In 2016, Russia waged an unprecedented and egregious campaign to undermine U.S. democracy. In January 2017, ODNI released a declassified report on Russian activities that stated the U.S. government had "high confidence" that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election" in order to "undermine public faith in the US democratic process, denigrate [Hillary] Clinton, and harm her electability and potential presidency."[13] The report also assessed that the Russian government "aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him."[14]

The January 2017 ODNI report and numerous rounds of recent testimony to Congress by experts on Russia have made clear that Russia's interference into the U.S. elections in 2016 was neither its first nor its only assault on a country's electoral system.[15] Both prior and subsequent to its 2016 assault on the U.S. election infrastructure, Russia conducted hybrid assaults on elections and democratic institutions in Ukraine, the Balkans and throughout Europe.[16] Russia has targeted the United States in the past as well, as the January 2017 ODNI report stated, noting "Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin."[17]

What was new in Russia's 2016 meddling was not its goal of undermining democratic values, or its targeting of election infrastructure, but rather that Russia's election interference was conducted on a massive scale and with a high level of technological sophistication. As the January 2017 report noted, "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[18]

Russia's campaign of election interference in 2016 included hacked e-mails and their distribution on WikiLeaks, fake and/or automated social media accounts, and false news stories. As U.S. intelligence agencies also reported in January 2017:

> "Russian intelligence obtained and maintained access to elements of multiple…state or local electoral boards."[19]

According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records and positioning themselves to carry out future

attacks.[20] In June, media also reported that the Russians accessed at least one U.S. voting software supplier and sent spear-phishing emails to more than 100 local election officials just days before 2016 November's presidential election.[21] Although in most of the targeted states officials saw only preparations for hacking, such as scanning of networks in Arizona and Illinois, voter registration databases were reportedly breached.[22]

> If 2016 was all about preparation, what more can they do and when will they strike?

While it is possible Russia's interference was a unique political event, experts warn that Russia and other state actors will almost certainly be back to seek to undermine our democracy in the future. For instance, when asked in March about the prospects for future interference by Russia, then-FBI Director James Comey testified before Congress that: "[T]hey'll be back. They'll be back in 2020. They may be back in 2018."[23] Commenting on Russia's extensive capability to hack into county and local databases, former DHS Secretary Jeh Johnson stated that even during the 2016 election he had feared Russia's possible targeting of state voter databases.[24] Furthermore, numerous security and intelligence experts have noted that we have significant reason to fear such an attack by Russia in the future.[25] Some have even voiced concerns that having suffered probing attacks last year, we may face an even more sophisticated assault next time around.[26] Russia retains all of the significant cyber capabilities it exhibited in 2016, and experts believe that the Russian government will have learned from its 2016 experience to more effectively exploit vulnerabilities going forward.

North Korea

North Korea has also long viewed cyber capabilities as tools to use against its perceived adversaries,[27] and could potentially launch a cyber operations against the United States' vulnerable election infrastructure. North Korea's cyber capabilities have improved steadily over time,[28] and could inflict significant damage on U.S. private or government networks.[29] Although debate continues about the precise scope and extent of North Korea's cyber capabilities, a high-ranking U.S. military official assessed in April 2014 that North Korea employed hackers capable of cyber-espionage and disruptive cyberattacks.[30]

Experts on the Democratic People's Republic of Korea (DPRK) have identified a range of motivations for North Korea to conduct cyber operations, including retaliatory attacks.[31] A prime example of North Korea's cyber hacking capabilities is the 2014 hacking of Sony Pictures Entertainment.[32] Recently, North Korean cyber actors appear to have begun significantly expanding their targeting of entities and institutions in various countries, including broadened attacks against government entities and private companies from the Republic of Korea[33] and financial institutions in the United States. The WannaCry ransomware infected as many as 300,000 users worldwide, including hospitals, and were caused by a strain of cyber worms that restricted users' access to a computer.[34] Experts have suggested that North Korean hackers were almost certainly behind this attack.[35] In a briefing on December 19, 2017, Tom Bossert, President Donald Trump's homeland security adviser, officially attributed the WannaCry ransomware to the North Korean government.[36]

The WannaCry hackers are also said to be part of the "Lazarus Group" that was also behind the February 2016 hacks of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging service.[37] The SWIFT system is used by some 11,000 banks and companies to transfer money from one

country to another and is considered the backbone of global finance.[38] The hacks of these SWIFT financial terminals resulted in the theft of approximately $81 million from banks in Bangladesh and Southeast Asia.[39] North Korea is now being linked by a number of cyber experts to similar attacks on banks in as many as 18 countries.[40] If confirmed, these techniques used would represent a troubling new capability.[41]

> North Korea, like Russia, has also shown it likely has the capability not only to hack and release e-mails, but also to alter data.[42]

Should the DPRK decide that creating election chaos is worth the risk of potential retaliation from the United States, North Korea could use its cyber capabilities to manipulate poll books stored online. If the DPRK can target financial networks, large corporations like Sony, and companies that are part of a country's energy network, then smaller, resource-strapped U.S. towns, counties, and states will have difficulty resisting or responding to a targeted attack. Experts assess that as pressure from the West to derail North Korea's nuclear weapons program increases, DPRK leader Kim Jong Un will likely continue to develop cyber capabilities in response.[43] Additionally, while experts have suggested that traditionally China could exert some degree of control over North Korean hackers' access to the internet, North Korea is actively exploring ways to circumvent such restrictions. A senior technology officer at a leading cybersecurity firm noted the DPRK's new connection to the outside world via Russia would enhance North Korea's ability to command future cyber operations.[44]

Iran

Iran has long had the United States in its political cross-hairs. Iran has heavily invested in building up the cyber capabilities of the Iranian Revolutionary Guard Corps (IRGC) and other Iranian government proxies.[45] Iran has also been scaling up its cyber capacities since the Stuxnet – a complex piece of malware designed to interfere with Siemens Industrial Control systems for nuclear centrifuges – was discovered in Iran[46] and elsewhere.[47] Under President Rouhani, Iran increased its cyber budget twelve-fold, which based on some assessments makes it a "top five world cyber-power."[48] Experts also point to Iranian cyberattacks on Wall Street as an example of the threat Iran poses to the broader U.S. civilian infrastructure. In fact, Fire Eye reported that of its investigations of attacks on Western companies and governments, Iran now ranks with China and Russia in terms of frequency of attack.[49]

Iran's most infamous cyber operations include the "Shamoon" attack on Saudi giant Aramco[50] and several waves of "distributed denial of service" attacks against at least 46 major financial institutions and companies and critical infrastructure.[51] Targets included six leading U.S. banks, including J.P. Morgan Chase.[52] The Justice Department indicted seven Iranian hackers for the coordinated financial services attacks, which included an attempt to interfere in the command and control system of a New York dam.[53] Separately, a September 2017 cyber security firm report identified a new Iranian-sponsored hacking group, nicknamed APT33, which has been targeting organizations in the aviation and energy industries in the United States, South Korea, and Saudi Arabia.[54]

As a result of the 2015 nuclear deal, Iran appears to have cut back on cyberattacks aimed at U.S. banks and government agencies.[55] However, prominent experts warn that Iran may decide to interfere in future U.S. elections as retribution for U.S. actions, particularly if Iran assesses there would be no significant U.S. response.[56] Moreover, in an example of Iran's ongoing

malicious activity, a Forbes investigation revealed that an employee at a major U.S. accounting firm, Deloitte, allegedly fell victim to a sophisticated fake Facebook account operated by Iranian hackers in late 2016.[57] This same Iranian hacker group's recent activities have provoked increased concern about Iran's possibility of ramping up its cyberattacks on the United States in response to the Trump Administration's stance on the regime.[58] Experts have raised concerns that rather than acting wholly on their own, hackers from the Iranian cyber army could team up with the Russians or other actors to pool capacity and resources to target the U.S. electoral system.[59]

> Experts have warned that Iranian hackers have relationships with the Russians, Chinese, and North Koreans, and have exchanged tactics, tools, and procedures for cyber warfare with at least Russia and North Korea.[60]

China

China has consistently been identified, along with Russia, as one of the most persistent and advanced cyber actors threatening the United States today. China has engaged in various cyber operations either for espionage or political motivations. Furthermore, China, together with Russia, tops the list of state actors that possess the most sophisticated capabilities and have also integrated their cyber tactics into their warfighting strategies and doctrines.[61]

Among the most infamous cyber intrusions commonly attributed to China are the hacks of the U.S. Office of Personnel Management (OPM).[62] China had previously been identified by the U.S. government as one of the most active state actors in cyberspace. For example, the United States filed criminal charges in May 2014 over a set of computer intrusions and indicted five members of China's People's Liberation Army (PLA).[63] Also, in May 2013, Chinese hackers reportedly compromised the computer systems of at least nine U.S. agencies, including the Department of Labor and the Army Corps of Engineers' National Inventory of Dams.[64] Also in 2013, a China-linked threat actor known as Deep Panda reportedly compromised high-tech sector companies, the U.S. defense industrial base, nongovernmental organizations, and state and federal government entities for espionage purposes.[65]

The debate about the threat China poses is not only about its capabilities, but also its motivations. In September 2015, China and the United States reached an agreement on refraining from conducting economic cyber-espionage. It is still too early to reach conclusions about China's activities, post-agreement. Nonetheless, experts have noted that, China unlike Russia, has to-date largely restricted its activities to espionage rather than interfering in U.S. elections on a grand scale.[66] Experts assess that China is also deeply concerned about and intent on preserving plausible deniability related to its cyber actions.[67] Therefore, China may not follow the Russian model of unabashed interference in the U.S. elections beyond hacking campaigns for espionage purposes.

> The most concerning issue is China's advanced cyber warfare capabilities could be rapidly deployed and used against the U.S. and our interests should their political motivations and calculations change.

ADMINISTERING ELECTIONS

FEDERAL AGENCIES

Although state and local officials are primarily responsible for administering and securing elections, certain federal agencies play a supporting role by setting security standards, administering grants for equipment upgrades, providing technical guidance and other resources, and promoting partnerships and information sharing among stakeholders.

The EAC is an independent, bipartisan commission that serves as a national clearinghouse of information on election administration. The EAC provides a vital link between state and local election administrators and the federal government by providing three main services: 1) testing and certifying voting machines; 2) assisting states with the management of election technology and 3) helping state and local officials prepare for elections.

DHS coordinates the overarching federal effort to promote the security, including cybersecurity, of the nation's critical infrastructure, defined as 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 thereof.[68] DHS also plays a key role in facilitating information sharing between federal, state, and local officials. Specifically, DHS is charged with analyzing and integrating law enforcement, intelligence, and other threat information, then disseminating such information, as appropriate, to federal, state, and local government officials with "responsibilities related to homeland security."[69]

These agencies have resources, expertise, and stakeholder relationships that can assist state and local election officials in securing their elections.

Election Assistance Commission

"The EAC was instrumental in providing us with key advice and counsel in the development of the Request for Proposals for new voting equipment and electronic poll books. The assistance ensured Rhode Island entered the 2016 election with state-of-the-art voting equipment."

- Nellie Gorbea, Rhode Island Secretary of State[78]

BACKGROUND AND ROLE

In the wake of the chaotic 2000 presidential election, Congress passed the Help America Vote Act of 2002 (HAVA). HAVA sought to improve election administration by instituting numerous reforms. Some of the most notable include: 1) providing funds to replace antiquated voting machines, 2) requiring states to create a computerized, statewide voter registration list, and 3) promoting accessibility for people with disabilities.

HAVA created the EAC to administer the newly created grant program, to develop guidance to assist states in meeting HAVA requirements, and to serve as a national clearinghouse of information on election administration. In addition, the EAC tests and certifies voting machines, provides guidance on managing election technology, and works with state and local officials to assist them in preparing for elections.

Testing and Certifying Voting Machines

The EAC tests, certifies, and decertifies voting machines to help states better navigate the voting machine procurement process. The voting machines are tested against a set of standards, the Voluntary Voting System Guidelines (VVSG), put together by the EAC in conjunction with the National Institute of Standards and Technology (NIST) as well as experts from the public and private sectors. The most recent VVSG were adopted in 2015. Currently, the VVSG are in the process of being updated, and the EAC anticipates adopting revised guidelines in the first half of 2018.[70] Though states are not required to participate in the EAC's testing and certification program, over 40 states currently require either certification or some component of the Commission's testing and certification program for the voting systems used in their jurisdictions.[71] Of the states that do not use any part of the EAC's testing or certification program, three (Florida, Oklahoma, and Oregon) were targeted by Russian hackers in 2016.[72]

Managing Election Technology

In addition to testing and certifying voting machines, the EAC has sought to assist election officials with the rest of the technology involved in running an election. In 2016, the EAC launched a video series that featured election officials, advocacy groups, and academics and offered guidance on how to leverage high and low-tech tools in administering elections.[73] The Commission also provides easy-to-follow cybersecurity guidance on protecting voter registration data and securing election night reporting systems.[74]

Helping State and Local Officials Prepare for Elections

The EAC seeks to be a useful resource to election administrators across the country. In anticipation of the 2016 election, the EAC launched an election preparedness campaign that provided guidance and materials to states on topics such as poll worker management, serving military voters, and running vote by mail programs. In 2016, the EAC produced 22 instructional and facilitative videos, nearly 100 blog posts, and ten public meetings, summits and round tables.

In 2016, as discussions concerning the security of elections and potential foreign interference became increasingly common, the EAC leveraged its existing relationships with election administration officials to facilitate communication between state election officials and the DHS.[75] EAC Commissioner Tom Hicks, when appearing before the Task Force at a public forum in October stated that, "The EAC has been a key player in helping election officials understand and leverage the Department of Homeland Security designation of elections infrastructure as critical infrastructure."[76] The EAC has facilitated, mediated, and participated in meetings between elections officials and DHS, and produced educational materials to help states understand and utilize the critical infrastructure designation. In addition, the EAC served as a resource to DHS to help the agency understand election administration.[77]

Over the past 15 years, the EAC has proven itself an important partner to state and local election officials. According to Rhode Island Secretary of State Nellie Gorbea, "The EAC was instrumental in providing us with key advice and counsel in the development of the Request for Proposals for new voting equipment and electronic poll books. The assistance ensured Rhode Island entered the 2016 election with state-of-the-art voting equipment.[78]

PATH FORWARD

Since 2011, Republicans have made several attempts to eliminate the EAC. In June 2011, a bill to terminate the Commission reached the House floor, but failed to gain enough votes to pass under suspension of the rules.[79] In addition, Congress has often stalled in confirming a full set of commissioners to the EAC. Between 2011 and 2015, the EAC did not have any commissioners as the Republican-lead Senate would not confirm nominees.[80] During this time, the EAC was unable to approve new

voting machine guidelines as three commissioners are required to act. As a result, some states were forced to delay purchasing new voting machines. Three commissioners were approved in 2015; however, the Commission still lacks a fourth commissioner.

The EAC operates on a small budget, spending between eight and ten million dollars in recent years. Given the vital role the agency plays in ensuring the integrity of our elections, Congress should be working to provide more resources. Not only does the agency provide the only federal voting machine testing and certification program, but it was also vital in protecting our elections in the face of foreign interference in the 2016 election. Former FBI Director James Comey, testifying before the Senate Judiciary Committee in May 2017, stated the following:

> In short, what we've done with DHS is share the tools, tactics, and techniques we see hackers, especially from the 2016 election season, using to attack voter registration databases and try and engage in other hacks. And we've pushed that out to all the states and to the Election Assistance Commission so they harden their networks. That's one of the most important things we can do.[81]

The EAC is in the unique position of being a federal agency with relationships with state and local election officials, and with an expertise in election administration. The Commission has been vital to helping states work with DHS to understand and take advantage of the "critical infrastructure" designation. Since the designation was made in January 2017, the EAC has worked diligently to build trust between state election officials and DHS by facilitating dialogue and drafting a white paper on critical infrastructure for state officials.[82]

Instead of attempting to terminate the agency, the President should nominate and the Senate should confirm a fourth commissioner, and Congress should work to provide the EAC with more resources so it can provide more robust assistance to states on election security issues. In February 2017, Rep. Robert Brady introduced legislation to reauthorize the Election Assistance Commission and to provide funds for the EAC to assist states with security upgrades for the voter registration systems.[83]

Department of Homeland Security

> In the years following DHS' formation, security experts warned that the "invisible enemy" could manifest as a major cyberattack that disrupts the networks we rely on for clean water, electricity, food, or medical care. Few anticipated that the looming "Cyber Pearl Harbor," would take the shape of a foreign adversary targeting U.S. election systems.

In its 2002 proposal to stand up the Department of Homeland Security, the Bush White House warned of "invisible enemies that can strike with a wide variety of weapons" and advocated for "a single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future."[84] The *Homeland Security Act of 2002* established the Department of Homeland Security, in part, to centralize national efforts to harden the defenses of vulnerable U.S. infrastructure and assets that could be exploited by our enemies and to help create a robust information sharing environment to remedy the shortfalls exposed in the 9/11 attacks.[85] For the 16 sectors of the U.S. economy designated 'critical infrastructure,' DHS is authorized to provide priority access to technical assistance, vulnerability assessments, access to information sharing centers and classified threat intelligence, incident response, and

other resources.[86]

In the years following DHS' formation, security experts warned that the "invisible enemy" could manifest as a major cyberattack that disrupts the networks we rely on for clean water, electricity, food, or medical care.[87] DHS organized its cybersecurity programs accordingly, focusing its limited resources on tools, technologies, and relationships that would help ensure continuity of operations for hospitals, telecommunications, and the electrical grid.[88] It primarily provides these services through its National Protection and Programs Directorate (NPPD). Few anticipated that the looming "Cyber Pearl Harbor," would take the shape of a foreign adversary targeting U.S. election systems.[89]

Critical Infrastructure

Critical infrastructure owners and operators enjoy priority access to a number of DHS cybersecurity programs and services, including cyber hygiene scans for Internet-facing systems, Risk and Vulnerability Assessments, and incident response assistance.[90] Owners and operators are also eligible to apply for security clearances, tap into classified information sharing exchanges, and participate in collaborative councils designed to foster a more enduring, consistent dialogue with other security stakeholders.[91] The designation also carries international significance. A 2015 United Nations agreement signed by 20 nations, including Russia, to refrain from conducting or supporting cyber-activity that intentionally damages or impairs the operation of critical infrastructure in providing services to the public.[92] The agreement also calls on nations to assist one another in defending their critical infrastructure against cyberattacks.[93]

Each sector has an assigned Sector Specific Agency (SSA) responsible for developing and implementing a Sector Specific Plan, a component of the National Infrastructure Protection Plan (NIPP) maintained by DHS.[94] DHS establishes a Government Coordinating Council (GCC) comprised of relevant public sector stakeholders, and sectors and subsectors may establish Sector Coordinating Councils (SCCs) for private entities. Although DHS may offer support upon request, SCCs are self-organized, self-run, and self-governed.

Information Sharing

To promote frank conversations between DHS, SSAs, and critical infrastructure owners and operators, federal law protects information on critical infrastructure vulnerabilities, or Protected Critical Infrastructure Information (PCII), from disclosure under the Freedom of Information Act and similar state statutes.[95] The designation also makes it easier for critical infrastructure stakeholders to share threat intelligence through platforms like the NPPD's National Cybersecurity Communications and Integration Center (NCCIC), a 24/7 watch center that collects, analyzes, and disseminates indicators of concern.[96] This information flows to critical infrastructure sectors through Information Sharing and Analysis Centers (ISACs), central nodes within each sector for communicating about cyber threats.[97] The Multi-State ISAC (MS-ISAC) performs this function for state, local, tribal, and territorial governments.[98]

It should be noted that DHS is not a regulator.[99] Participation in DHS' programs is voluntary, and their success relies on stakeholders choosing to participate both for their own benefit and the greater good of the sector. DHS brings to bear an ability to build and convene a robust network of critical infrastructure security stakeholders and provide an apparatus for sharing threat intelligence, candidly discussing vulnerabilities, and fostering public-private cooperation.[100] When DHS detects malicious activity or learns of a breach, it may notify the owner or operator of the affected system.[101] However, owners and operators are ultimately responsible for securing their systems and assets.

DHS EFFORTS IN THE 2016 ELECTION

"Time is a factor..."[123]

DHS entered the election security arena in the summer of 2016 when, in the wake of the cybersecurity breaches targeting political candidates and institutions, the NCCIC began receiving reports of cyber-enabled scanning and probing of state election-related infrastructure, some of which appeared to originate from a server operated by a Russian company.[102] Around this time, DHS also began fielding inquiries from Members of Congress, including Rep. Bennie G. Thompson, who wrote to DHS in early August to urge the Secretary to "act swiftly" to "defend the integrity, reliability, and validity of our free and democratic elections." The letter went on to note that "DHS, as the federal government lead for working with State, local, tribal, and territorial governments to secure critical infrastructure and information systems, is the natural partner for efforts to address cyber vulnerabilities in the nation's electoral system."[103]

On August 3, 2016, DHS made its cybersecurity and infrastructure protection capabilities available to state and local election officials and engaged in an outreach campaign to persuade stakeholders to use them.[104] Specifically, DHS contacted election community stakeholders like the EAC and the National Association of Secretaries of State (NASS) to offer cybersecurity assistance, make them aware of an FBI alert related to breaches into two state election boards, and urge them to check their systems for similar activity.[105] In order to facilitate the delivery of DHS' voluntary cybersecurity services, Secretary Johnson began considering designating election systems as critical infrastructure.[106]

On August 15, 2016, Secretary Johnson brought the EAC, NIST, and DOJ together for a conference call with NASS and other organizations representing state chief election officials. Recognizing the need to streamline information sharing with the elections community, Secretary Johnson announced plans to stand up an Election Infrastructure Cybersecurity Working Group.[107] Despite some initial criticism for not including representatives from the tech community, this working group served as a focal point for coordination between DHS and election administrators in the lead-up to Election Day and thereafter.[108]

Secretary Johnson made another push to state officials to implement cybersecurity recommendations from NIST and EAC and invited them to take advantage of DHS' suite of free, voluntary cybersecurity tools and services.[109] Some of the most relevant services included:[110]

Cyber Hygiene Scans, which can be conducted remotely and, therefore, more quickly than other services. Through these scans, DHS is able to generate a report for state and local officials identifying vulnerabilities and recommend security measures for online voter registration, election night reporting, and other Internet-connected systems.

Risk & Vulnerability Assessments, a more thorough, on-site review conducted by DHS cybersecurity experts. RVAs typically require two to three weeks and include a wide range of internal and external vulnerability testing services, concluding with a full report on vulnerabilities and recommended mitigation measures.

Incident Response Assistance in the event of suspected malicious cyber activity. State and local election officials were advised to report such activity to the NCCIC, which could, upon request, provide on-site assistance in identifying and remediating a cyber incident. This information could then be shared with other states to help them defend their own systems.

Information sharing, primarily through the MS-ISAC, a platform for sharing threat intelligence with state officials, usually the state Chief Information Officers (CIOs). Cleared stakeholders could receive classified briefings upon request.

Field-based cybersecurity and protective security advisors who can provide actionable information

and connect election officials to a range of tools and resources available to improve the cybersecurity preparedness of election systems and the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management assistance for both cyber and physical incidents.

Physical and protective security tools, training, and resources to improve security at polling sites and other physical election infrastructure. At the time, DHS provided specific guidance for administrative and volunteer staff to identify and report suspicious activities, active shooter scenarios, and other threats.

Secretary Johnson also discussed ongoing deliberations about whether to designate election systems as critical infrastructure.[111] Reactions varied, particularly because DHS did not suggest additional funding would accompany the critical infrastructure designation.[112] DHS also struggled to combat the perception that requesting DHS cybersecurity assistance amounted to a federal takeover of elections. In any event, by that point there was insufficient time for state election officials to make any significant changes to elections systems to resolve any new vulnerabilities identified[113] and states were increasingly concerned about undermining confidence in the election process.[114]

On August 5, 2016, NASS issued a statement confirming that state officials would be vigilant in their efforts to secure election infrastructure, but that "there has been no indication from national security agencies to states that any specific or credible threat exists when it comes to cyber security and the November 2016 general election."[115] Ultimately, it deemed "hacking of the election is highly improbable due to [the] unique, decentralized process."[116] Nevertheless, NASS said its members would engage in ongoing information sharing with the federal government related to cybersecurity risks and how to address them,[117] while working to educate Congress and the public about its ongoing election security efforts and the need to invest and recapitalize voting technology.[118]

DHS was slow to gain the trust and buy-in of its state partners. On September 28, 2016, with the election nearing and fewer than half the states requesting assistance from DHS, bipartisan Congressional leadership wrote to state election officials to urge them to take advantage of resources to secure their network infrastructure, including those offered by DHS.[119] At the same time Congressional leadership promised to "oppose any effort by the federal government to exercise any degree of control over the states' administration of elections by designating these systems as critical infrastructure."[120]

> "Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company."[121]

On October 7, 2016, one month before Election Day, Secretary Johnson again urged state officials to take advantage of DHS cybersecurity assistance to secure their election systems in light of intelligence related to Russian efforts to meddle in the 2016 presidential election. That day, DHS and ODNI released a Joint Statement announcing with confidence that the Russian government was behind "compromises of emails from US persons and institutions, including from US political organizations." Additionally, the statement revealed that some states had "seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company."[122]

On October 10, DHS once again warned election officials that: "[T]ime is a factor… There are only 29 days until Election Day."[123] Although cyber hygiene scans can be performed quickly and remotely, "it can take up to two weeks…to run the scans and identify

vulnerabilities. It can then take at least an additional week for state and local election officials to mitigate any vulnerabilities on systems that we may find."[124] With consistent prodding, DHS provided cyber hygiene scans to election officials in 33 states and 36 local jurisdictions and shared over 800 cyber threat indicators officials could use to identify attempted intrusions, as well as other tactics, techniques and best practices, with officials in thousands of jurisdictions across the country.[125]

CRITICAL INFRASTRUCTURE DESIGNATION

> "We should carefully consider whether our election system, our election process is critical infrastructure, like the financial sector, like the power grid...There's a vital national interest in our electoral process."
>
> *- Jeh Johnson, Former Secretary of the Department of Homeland Security*[126]

After Election Day, evidence continued to surface about the extent of Russian interference. DHS worked with the Intelligence Community to carry out a broad review of all election-related hacking incidents before the end of the Obama Administration.[127] On December 29, the day President Obama announced sanctions against Russia, DHS, ODNI, and the FBI released a Joint Analysis Report (JAR) titled Grizzly Steppe – Russian Malicious Cyber Activity offering greater detail about Russian targeting and urging owners and operators to look back at their network traffic for signs of malicious activity.[128]

On January 6, 2017, the U.S. Intelligence Community reported that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election" and Russian intelligence attempted to breach multiple state or local election boards.[129] According to the report, "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[130] Russia's long-standing, multi-faceted strategy "blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls' in order to cripple its adversaries."[131]

That same day, then-Secretary Jeh Johnson designated election infrastructure as critical infrastructure.[132] In making the designation, then-Secretary Johnson stated:

> I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.
>
> I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities.[133]

Importantly, then-Secretary Johnson made clear that a State or local election board's decision to avail itself of DHS' cybersecurity resources is voluntary: "This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country."[134] The designation requires the Department "to prioritize our cybersecurity assistance to state and local election officials, but only for those who request it."[135]

Regardless, the announcement escalated tensions between DHS and the elections community and re-

Former Secretary of Homeland Security Jeh Johnson and former Under Secretary for the DHS National Protection and Programs Directorate Suzanne Spaulding testifying before the Task Force on September 28, 2017. Both officials warned that Russia will continue to target western democratic elections and urged swift action to secure U.S. voting systems.

ignited concerns about federal overreach. NASS issued a resolution opposing the designation, describing it as "legally and historically unprecedented, raising many questions and concerns for states and localities."[136]

Since January 2016, DHS has worked with election officials to help them understand and take advantage of the designation. However, the reception within the election community has continued to be mixed. In June, DHS announced it was "beginning the formal process of engaging election officials on an ongoing basis around the country" by participating, alongside the FBI and EAC, in the NASS annual conference.[137] At that conference, DHS sought to provide clarity about the designation and announced that DHS was "expanding its efforts to ensure state and local election officials can access the sensitive data, cyber tools and threat assessments they need to lock down their voting systems prior to the 2018 elections."[138]

After the conference, state officials said they were "disappointed" that DHS officials "weren't prepared to answer our questions" and frustrated that DHS was still only able to have surface-level conversations about the designation.[139]

Specifically, election officials expressed great frustration with DHS' information sharing practices.[140] Although DHS officials testified in June 2017 that Russia targeted voting systems in 21 states, for example, it did not notify state election officials whether their election systems were targeted until late September, almost a year after the election.[141]

In part, DHS attributed these information sharing challenges to the nature of its existing information sharing channels and reporting structures within each state.[142] As a general rule, DHS shares threat information at the state level through state Homeland Security Advisors, Fusion Centers, CIOs and other agents of the

state Governor.[143] Each state government is organized differently but, for the most part, Secretaries of State and other chief election officials are independently-elected officials who do not report to the Governor and exist outside the executive branch chain-of-command. As a result, information shared by DHS did not automatically flow to them under existing information-sharing relationships.[144]

The separation of voting systems from state networks that operate within a governor's chain-of-command has another important implication. Because of their political independence, Secretaries of State and election directors often maintain their own networks, instead of relying on the statewide networks that support other state agencies. These statewide networks are generally protected by DHS-provided sensors, known as Albert sensors, which are deployed to entities that participate in the MS-ISAC to monitor web traffic and detect malicious activity. As a consequence, depending on the governance model in a given state, these DHS sensors may not have been monitoring the state's election-related networks. Traffic from Albert sensors feeds into the MS-ISAC, giving DHS some visibility into malicious activity on the statewide network – but not necessarily the separate networks that support voting systems.

The elections community also struggled to reconcile the benefits DHS promoted as part of the critical infrastructure designation and the timeliness with which these services could be delivered. For instance, although DHS promised access to classified intelligence and other information about threats, election officials quickly learned that they would first need to undergo a lengthy security clearance process.[145] Although DHS assured state representatives that the clearance issue was being worked out internally, DHS has only begun the clearance process for state election officials and was slow to communicate the process for requesting a clearance.[146] Election officials also had difficulty squaring DHS' offer of 'priority access' to services with the nine month waiting list for certain services like Risk and Vulnerability Assessments.[147] These delays render the benefit useless in light of the compressed time frame of an election cycle.

DHS has also struggled to build relationships with and communicate information to the close-knit elections community.[148] For instance, despite DHS being fairly open that it is not the subject matter expert on election administration, it is currently serving as the SSA for the Elections Subsector. Although EAC has a breadth of expertise and long-standing relationships within the elections community, DHS has historically selected executive agencies to serve as SSAs because it preserves the executive prerogative to direct and guide the SSAs activities. The EAC is an independent agency and, accordingly, does not operate under direction from the president. This is a challenge for DHS, which lacks both institutional knowledge about election administration and connections within the small, close-knit elections community. As a result, DHS has leaned heavily on EAC for technical expertise and goodwill with elections stakeholders and is working with EAC to finalize the terms of a Memorandum of Understanding or other instrument that would formalize the agency's role in subsector activities.

Compounding existing challenges related to its election infrastructure responsibilities, DHS officials have testified that they are struggling to meet the surge in demand for these services since the designation, and the Office of Cybersecurity and Communications is diverting resources from other programs to meet demand.[149] Additionally, although DHS' September 2017 outreach effort to provide state election officials information regarding whether their infrastructure was targeted appeared to be well-executed, some states ultimately questioned the veracity of the information DHS provided.[150] The following week at least two states reported that DHS had clarified that the targeting occurred against other state networks, not elections systems. DHS maintained that Russian actors could have scanned other state systems in an effort to find

vulnerabilities that could be used to breach election systems.[151] Whatever the reason, these communications hiccups undermined DHS' efforts to build trust within the elections community.

To address these deficiencies, DHS officials say they are engaging in "unprecedented outreach" to "[enhance] awareness among election officials, [educate] the American public…develop information sharing protocols and establish key working groups to address these challenges."[152] DHS is also reportedly planning to dedicate more resources to election cybersecurity by elevating DHS' elections work out of the NPPD and into a new Department-wide Task Force.[153]

PATH FORWARD

> "[Election security] is my top priority at the Department. [If] we can't do this right, if we can't dedicate every single asset we have to assisting our state and local partners, then frankly...I am not sure what we are doing day-to-day...we are prioritizing delivery of those briefings, information sharing to our state and local partners...That for me is the No. 1 priority for NPPD from a critical infrastructure perspective...We cannot fail there."
>
> *-Christopher C. Krebs, Senior Official Performing the Duties of the Under Secretary of NPPD*[154]

Although DHS has struggled to build trust with Secretaries of State and other entities within the close-knit election administration community, the Department is beginning to make progress executing its responsibilities associated with the critical infrastructure designation. The Elections Government Coordinating Council (EGCC) held its first meeting in October and plans to use the forum to address governance and information-sharing protocols.[155] The Subsector plans to begin convened the first Sector Coordinating Council in December 2017, and will meet again in January 2018.

The Department has also acknowledged the urgency of addressing information sharing challenges and, although they have not committed to a specific strategy for disseminating information to election officials, they are conducting a pilot with the MS-ISAC and a sample of states. DHS also hopes the elevation of election security operations to a Department-wide task force will make it easier to dedicate resources and expedite access to cybersecurity services.

Overall, DHS officials have emphasized the Department's commitment to the election security mission. Testifying before a Congressional Subcommittee, the Senior Official Performing the Duties of the Under Secretary of NPPD stated that: "[Election security] is my top priority at the Department. [If] we can't do this right, if we can't dedicate every single asset we have to assisting our state and local partners, then frankly…I am not sure what we are doing day-to-day…we are prioritizing delivery of those briefings, information sharing to our state and local partners…That for me is the No. 1 priority for NPPD from a critical infrastructure perspective… We cannot fail there."[156] DHS should continue to partner with the EAC, an agency that has longstanding relationships with state and local officials, to work to build trust with state and local election officials.

STATE AND LOCAL GOVERNMENT

There are nearly 7,000 election jurisdictions and over 100,000 polling places in the United States.

The Constitution gives states broad authority to determine the "times, places, and manner of holding elections" and gives Congress the authority to "make or alter" state election regulations.[157] In practice, election administration in the United States is decentralized. States and localities are in charge of running elections, although Congress has passed legislation setting guidelines on voter registration and voting systems through the National Voter Registration Act of 1993 and the Help America Vote Act of 2002 respectively.

Each state has a chief election official, and elections are often further decentralized with counties and localities administering the election. There are nearly 7,000 election jurisdictions and over 100,000 polling places in the United States.[158] States, and sometimes localities, purchase their own voting equipment and set their own rules on registering voters, counting ballots, and conducting recounts.[159] In addition, states are responsible for recruiting and training poll workers. Poll workers are on the front lines of elections, and serve as the link between election officials and voters. They often receive low pay and limited training, but they are vital in ensuring that Election Day runs smoothly.[160] States also devise and implement their own security measures.

States and localities have taken a variety of steps to secure their elections – many states have replaced paperless voting machines, hired IT staff, and regularly backup their voter registration databases.[161] States and localities expend significant resources to make sure that eligible voters are able to exercise their fundamental right to vote. The CalTech/MIT Voting Technology project estimated that the 2000 election cost states and localities $1 billion dollars to administer, or approximately $10 for each ballot cast.[162] The federal government should protect this investment, and help states ensure that our elections are secure.

Respecting that states run their own elections, the co-chairs of the Congressional Task Force on Election Security sent a letter on August 1, 2017 to the NASS, the National Association of State Election Directors, and the chief election official in each state, seeking information on where states could use assistance securing their elections. The letter solicited input from the Secretary of State or chief election official on the state's: 1) top five goals and priorities for the federal government with respect to election security; 2) the challenges encountered in updating and securing election systems; 3) how to make existing voluntary partnerships with DHS and the EAC most useful; and 4) what role Congress can play in securing elections. A summary of the key findings from our survey and other conversations with election officials follows:

States Need Federal Funding to Bolster Security Efforts

> "Congress needs to ensure that sufficient federal funding is available for states to procure and maintain secure voting equipment and increased security of all election systems. That needs to be an ongoing commitment, and not the one-time infusions of resources."
>
> *-Edgardo Cortés, Virginia Election Commissioner* [167]

The National Association of Secretaries of States, as well as every state that responded, highlighted the need for federal funds to assist states with safeguarding their election infrastructure. Specifically, most states indicated that federal funds were needed to replace aging voting machines.[163] In addition, respondents proposed several other ways that additional funding could help improve their state's election security including hiring an election technology security officer,[164] bringing in third party security firms to conduct vulnerability assessments,[165] and upgrading voter registration and election night reporting systems.[166]

Often, states and localities are unwilling or unable to provide funds for election infrastructure. Commissioner Edgardo Cortés told the Task Force of his experience in Virginia where he tried unsuccessfully to get state or local funding for the replacement of paperless voting machines that he knew to be error prone and vulnerable to cyberattack. He went on to say, "Congress needs to ensure that sufficient federal funding is available for states to procure and maintain secure voting equipment and increased security of all election systems. That needs to be an ongoing commitment, and not the one-time infusions of resources."[167]

There is still over $300 million of HAVA funding that remains to be appropriated, and Congress should act to make those funds available to states. In a letter to the Task Force, NASS has emphasized this point, "States would clearly benefit from the appropriation of the outstanding balance of federal HAVA funds to aid them in ensuring that they have sufficient equipment, technical support, and resources to maintain a sound security posture for their computer-based systems."[168] The Task Force recommends that the remaining HAVA funding be used for states to replace paperless machines with paper-based voting systems.

Congress Should Support the EAC and DHS

State election officials report that the EAC has been a valuable partner, and urged Congress to continue supporting the agency's work.[169] Though Republicans in Congress have made efforts to terminate the EAC, state election officials in traditionally Republican states have offered support for the Commission. Secretary Gale of Nebraska suggests "retaining the [EAC] to continue to provide election-related guidance and information to state and county election officials" and Marci Andino, the Executive Director of the South Carolina Elections Commission recommends expanding the role of the EAC.

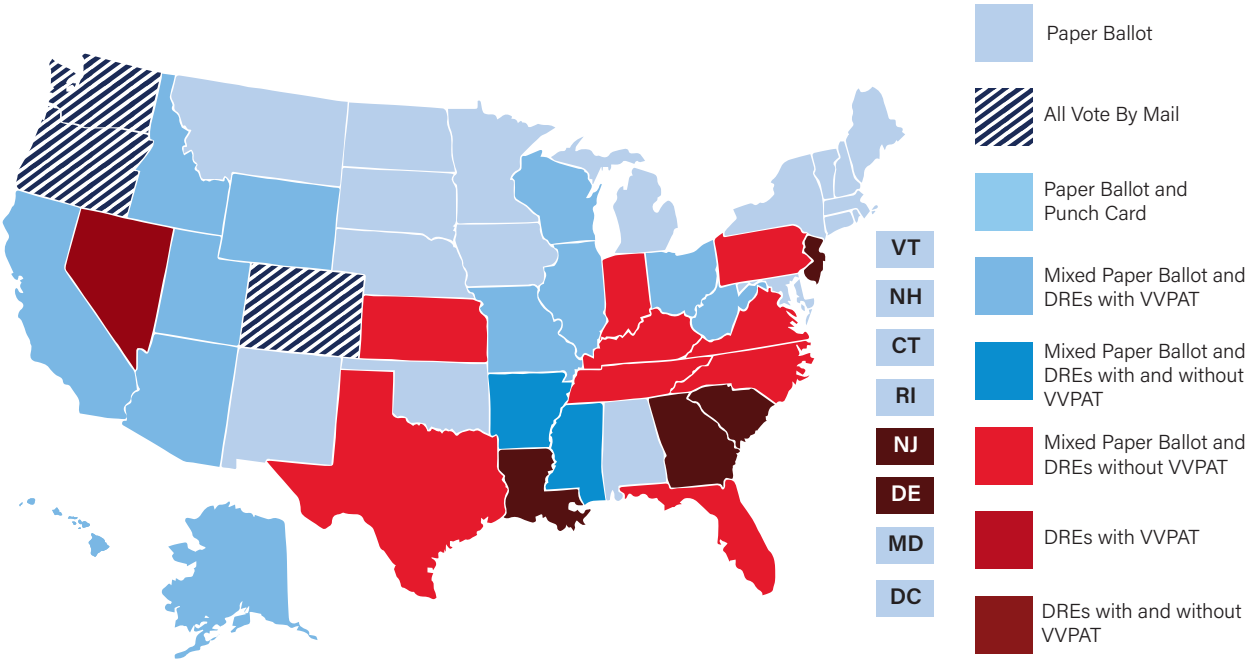
States also indicated that they found DHS' services to be helpful, particularly the Risk and Vulnerability Assessments offered by the agency. However, several respondents indicated that it would be helpful if DHS could reduce the amount of time states must wait to receive an assessment.[170] In addition, states suggested that the partnership between DHS and election officials could be improved by providing security clearances in a timely manner to at least one election official in each state.[171]

Finally, several states told us that it would be useful for the federal government to provide more guidance on voting system standards and best practices for securing and auditing both cyber and physical assets.

The Task Force has seen a great deal of support for these recommendations beyond the responses we received from state election officials.

The National Association of Counties (NACO) wrote a letter to Senator Mitch McConnell, Senator Chuck Schumer, Senator John McCain, and Senator Jack Reed, urging that they support S.A. 656 ("Klobuchar-Graham") that would have provided funding to states and localities for election security. NACO writes, "Counties are on the front lines of administering the nation's elections, and county election officials must address security issues daily. This amendment would provide vital and necessary resources for states and counties to meet the growing security demands of administering elections."[172] The letter went on to say that NACO also strongly supports the work of the EAC.

In addition, ten Secretaries of State wrote to Senator John McCain and Senator Jack Reed in support of Klobuchar-Graham. The letter was signed by both Republican and Democratic Secretaries who wrote, "This amendment would provide vital and necessary resources to support the growing technology and infrastructure security demands of our nation's elections."[173]



DRE: Direct Recording Electronic Voting Machines
VVPAT: Voter Verified Paper Audit Trail Printers
BMD: Ballot-Marking Device or System

This map shows the types of polling place equipment used across the country as of November 2016. Many states continue to use DRE and VVPAT technology that does not leave a reliable, auditable paper trail.

Verified Voting. "The Verifier – Polling Place Equipment – November 2016." Verified Voting, https://www.verifiedvoting.org/verifier/

FINDINGS

OUR ELECTION INFRASTRUCTURE IS VULNERABLE

The Help America Vote Act (HAVA) gave states over $3 billion dollars to upgrade and modernize their election infrastructure in the wake of the 2000 presidential election. Because of this investment in our election infrastructure, over 850 million ballots have been cast in federal elections since 2000.[174] For $3.50 per ballot, the federal government was able to ensure that eligible citizens could exercise their right to vote.

However, the lifespan of much of the hardware and software that was purchased with HAVA funding is between ten and fifteen years, and many jurisdictions are now using equipment that is nearing or past its useful life.[175] States and localities need federal assistance to invest in modern, secure election infrastructure. Congress should help immediately. HAVA authorized $3 billion to be spent on election infrastructure, and approximately $300 million remains to be appropriated. Those funds should be appropriated so states can begin to replace their most vulnerable voting systems.

Voting Machines

The Task Force's research and interviews unequivocally show that many jurisdictions are using voting machines that are highly vulnerable to an outside attack. Forty-two states are using voting machines purchased more than ten years ago.[176] Old machines are susceptible to "vote-flipping" (i.e., when a voter presses Candidate A's name, but Candidate B's name is selected on screen) and crashing which can sow doubt in voters' minds and give the impression that an election is being rigged.[177] Though many election officials would like to replace these machines, few have the money in their budgets to purchase new machines.[178] At the same time, when machines begin to break down, election officials are sometimes unable to find replacement parts as some parts are no longer manufactured.[179] As a result, election officials are turning to stop-gap measures like stockpiling replacement parts or buying necessary parts from eBay.[180]

In addition to the hardware vulnerabilities, many of these aging machines are running unsupported software. These machines rely on operating systems like Windows XP or Windows 2000 which pose a particularly significant security risk as those operating systems either do not receive regular security patches, or have stopped receiving support altogether.[181]

Some will defend the security of election systems by arguing that voting systems are secure because they are not connected to the internet. However, many voting machines contain software or hardware that could be used to connect to the internet.[182] In addition, many machines use removable memory cards or USB sticks to program their machines with ballot data, and it is possible to infect a memory card with malware that could crash a machine or alter vote totals.[183] A hacker could exploit the memory card vulnerability in a few different ways. First, an attacker could physically access the machines. While this may seem unlikely, voting machines are sometimes left unattended in polling stations in the days leading up to an election.[184] A greater threat, however, comes from outside vendors. The Brennan Center reports that a relatively small number of outside vendors can be responsible for programming the memory cards for multiple counties in a state.[185] For example, according to Professor J. Alex Halderman, Director of the University of

Michigan's Center for Computer Security and Society, "In Michigan, 75% of counties use just two 20-person companies to do that programming."[186] As discussed below, outside vendors are not subject to any federal regulatory requirements that would ensure they use cybersecurity best practices.

Given the breadth of security risks facing voting machines, it is especially problematic that approximately 20% of voters are casting their ballots on machines that do not have any paper backup.[187] These voters are using paperless Direct Recording Electronic (DRE) machines that have been shown over and again to be highly vulnerable to attack. Because these machines record votes on the internal memory of the machine, and do not leave any paper backup, it is near impossible to detect whether results have been tampered with.[188] In fact, in September of this year, Virginia decertified its DRE machines because of the security risks they present.[188] In addition, a group of over 100 computer scientists and cyber experts wrote to Congress asking that paperless DRE machines be phased out of use.[190] Paperless DRE machines are still in use in thirteen states, and the Brennan Center estimates that the cost to replace these machines would be between $130 and $400 million.[191] This estimate would only cover paperless DRE machines and does not include the cost of replacement of the DREs with a voter-verified paper audit trail (VVPAT) described below.

Some DRE machines have a VVPAT that allows voters the opportunity to review a printout of their selections before casting a ballot. However, the VVPAT system has two flaws. First, voters are unlikely to actually review the paper record to make sure it is accurate. Second, votes are still recorded on the internal memory of the machine. That means a hacker could infect the machine in a way where the paper printout reflects the voter's actual preference, but the machine's internal memory records a different vote. In other words, the printout does not necessarily verify whether the machine is tabulating correctly.[192] Moreover, in the process of implementing risk-limiting audits (described below), Colorado has found that VVPAT systems create significant logistical hurdles and are much harder to audit than paper ballots.[193] As a result, several experts we spoke to believe that the VVPAT machines should be phased out as well.[194]

The ease with which our voting machines can be hacked was demonstrated in July at DefCon, one of the world's largest, longest-running, and best-known hacker conferences. DefCon featured a Voting Machine Hacking Village ("Voting Village") which made 25 pieces of election equipment, including paperless electronic voting machines, available to hackers. The organizers of the Voting Village report, "By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems."[195]

The best way to determine whether a machine has been hacked, or mis-programmed, is to conduct a post-election, risk-limiting audit. Currently, 33 states and the District of Columbia require post-election audits of paper records; however, many experts note that many of those audits are insufficient to determine whether election results were tampered with.[196] Instead, experts recommend that states implement risk-limiting audits. A risk-limiting audit is a process that involves hand counting a certain number of ballots, using advanced statistical methods, to determine with a high degree of certainty that the reported election outcome is accurate. The number of ballots that are counted by hand is determined by many factors, including the margin of victory in the election. If the initial count determines that the election results are accurate, the audit stops. If the initial count is insufficient to confirm the election result, a larger sample of ballots is hand counted. This process continues until the election results can be confirmed. If

there is never enough evidence to confirm the election results, a full hand count would be conducted.[197]

Robust, statistically sound, post-election audits would enable election officials to detect any incorrect election outcomes.[198] When testifying before the Senate Intelligence Committee earlier this year, Professor Halderman stated that, "By manually checking a relatively small random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome was correct."[199] According to Professor Halderman, currently only New Mexico and Colorado are conducting such audits,[200] though Rhode Island recently passed legislation providing for post-election risk-limiting audits beginning in 2018 and requiring post-election risk-limiting audits beginning in 2020.[201]

Voter Registration Databases

HAVA requires states to create and maintain a statewide, computerized voter registration database.[202] According to the Brennan Center, in at least 41 states, these systems were created at least ten years ago.[203] The 2016 election has shown us that these systems are vulnerable to attack. The Department of Homeland Security found that Russian hackers targeted these systems in 21 states.[204] In Illinois, Russian hackers successfully breached the databases and attempted, but failed, to alter and delete voting records.[205] In Arizona, hackers were able to successfully install malware on a county election official's computer. That gave the hackers access to the official's credentials which could have then been used to get into the county's voter registration database.[206] In addition, hackers targeted at least one election vendor with the hope of ultimately obtaining access into voter registration databases.[207]

The most significant threat posed by vulnerable voter registration databases is that an attacker could alter, delete, or add voter registration records which would then cause profound chaos on Election Day and potentially change the results of the election. Had the attackers successfully changed voting records in Illinois, voters would have arrived at the polls on Election Day to discover that they were not registered. This could lead "scores of voters to cast provisional ballots, leading to long lines, undermining faith in the fairness of an election, and creating a major administrative headache to accurately count votes after the polls closed."[208] Alternatively, an attacker could add fake voters to the rolls, allowing for fraudulent votes to be cast.

States take many steps to secure their voter registration systems. Almost all states make a daily, offline copy of the statewide voter registration database.[209] In addition, states and counties each keep lists that can be used as backup for one another in the event of a breach. Numerous states took advantage of DHS "computer hygiene" screenings in advance of the 2016 election, and states are continuing to work with DHS and utilize the Department's services as election infrastructure is now a "critical infrastructure" sector.

Decentralization

The decentralization of American elections is both a strength and a challenge in this space. Because of the decentralization, some argue that a hacker cannot have one successful breach and then access the entire country's voting records. While there is certainly truth to that contention, there are ways in which our system is less decentralized than commonly thought. First, the election technology industry is increasingly consolidated with just a few firms serving most of the country.[210] Second, there are considerable supply chain vulnerabilities as many machines have foreign-made internal parts.[211] A report on the DefCon Voting Machine Hacking Village states, "[A] hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line. With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility."[212]

Having nearly 7,000 election jurisdictions means that each of those needs to have strong IT support to prevent against attack. Several election officials told the Task Force that they would greatly benefit from the federal government providing a centralized set of a guidance documents on cybersecurity best practices.[213] While the EAC provides guidelines for voting machines, they do not provide a similarly comprehensive set of guidance for voter registration systems.

In addition, states need better IT support and resources to help improve their cybersecurity infrastructure, though several states have been able to make progress in these areas.[214] In California, Governor Jerry Brown signed a law that will alert voters when their registration has been changed.[215] Colorado has added national guard security experts to its election team,[216] and Virginia recently created a digital security position.[217] In June, Governor Cuomo directed the New York State Cyber Security Advisory Board to review the security of New York's election infrastructure.[218] For the first time, Arizona has updated its election official training to include cybersecurity.[219] In October, Rhode Island Secretary of State Nellie Gorbea told the Task Force: "In Rhode Island, I have increased my office's IT staff by 40% to ensure that we have the technical expertise in-house necessary to respond to the ever-shifting landscape that technology presents."[220]

However, states still face several challenges when it comes to hiring the necessary IT staff and strengthening their networks. While some election officials are able to use state IT security experts to harden their systems,[221] in many other states, elections are run off of a different network than the state network, and state chief information officers are reluctant to assist the elections officials if they are not already existing customers of state IT.[222] This means that election officials will need to hire their own IT staff, and many simply do not have the money. [223]

While some in Congress may argue that states and localities should fund these improvements, states are struggling to find that funding. In most states, legislatures are not increasing their election security budgets.[224] In some cases, Governors are actively undermining election security efforts. In Florida, Governor Scott's budget proposed reducing the funding for the Division of Elections by almost one million dollars.[225] In July, Governor Kasich vetoed a provision in Ohio's budget that would have allocated one million dollars towards voting equipment.[226] Governor Walker issued a partial veto to the state's budget, and in doing so, eliminated five jobs from the Wisconsin Elections Commission.[227] This issue is simply too important to sit back and watch state governments and the federal government pass responsibility back and forth. A sovereign nation attacked 21 states, and the federal government should provide the funds necessary for states to defend themselves.

STATE AND LOCAL GOVERNMENTS NEED FEDERAL SUPPORT TO REPLACE OBSOLETE ELECTION SYSTEMS

There is no question that securing election infrastructure and preserving public confidence in election outcomes are the top priorities of state and local elections officials. It is also clear that these officials are aware that much of the technology upon which they rely to administer elections is outdated or obsolete and must be replaced. That much has been made clear by the NASS, former federal officials, and individual Secretaries of State. Moreover, it is similarly clear that the ability of state and local election offices to maintain staff with relevant expertise to develop and implement cybersecurity programs necessary to secure election systems is inconsistent across the nation.

The crisis-to-crisis model of federal investment in election infrastructure and security capabilities has resulted in avoidable vulnerabilities in our elections systems. Despite being well-aware that outdated election systems must be replaced, state and local budgets are already stretched thin. If Congress expects State and local election officials to replace, maintain, and secure election systems, it must help absorb both immediate and long-term costs. This includes providing money for innovation grants that will help keep our election system secure in the face of evolving threats.

FEDERAL AGENCIES LIKE DHS AND EAC NEED RESOURCES AND CONSISTENT SUPPORT FROM CONGRESS

Election Assistance Commission

The EAC provides a valuable service in issuing the VVSG and in testing and certifying voting machines. Despite these services being voluntary, nine states and the District of Columbia require that voting machines be tested to federal standards, seventeen states require testing by a federally accredited lab, eleven require full federal certification, and four additional states refer to standards set by federal agencies or standards.[228] The most recent guidelines were adopted on March 31, 2015, and they are currently in the process of being updated. The updates currently under consideration would greatly improve election security by requiring that machines have an auditable paper trail and that voting machines provide mechanisms to detect malicious activity.

These security updates are sorely needed and will greatly assist in safeguarding our voting machines. The EAC has indicated that they plan to adopt these guidelines in the first half of 2018, but given the urgency of the issue, every effort should be made to expedite this process. However, it is important to note that these guidelines are prospective and will only affect machines that are acquired after the guidelines are adopted.[229] The best way to ensure that states are using safe, reliable voting machines is for Congress to provide funding to help states replace old equipment with new machines that conform to the latest guidelines.

Creating standards for voting machines is a good start, but it is not enough. As discussed elsewhere in this report, the vulnerability of voter registration databases and other election administration software also present a significant threat, and it would be useful if the EAC would provide assistance in these areas as well. The EAC makes available on its website a checklist for securing voter registration databases and election night reporting systems.[230] These documents are easy to follow and great resources for state and local election officials. The EAC should work with experts in cybersecurity and election administration to ensure that these documents are up to date, and should work to publicize the availability of these documents.

While many election officials we spoke with commented on the EAC's testing and certification program, the EAC can and should provide additional cybersecurity resources to states.[231] Rhode Island Secretary of State Nellie Gorbea emphasized that states are already in the habit of turning to the EAC for election related resources, "Every single time that we are looking at doing something in cybersecurity, in elections administration, and improving things, we look at the EAC. Because they have all this information about what is happening at the national level. We absolutely need those resources there at the state and local level."[232] The existing relationship between the EAC and state and local election officials has led some officials to indicate that they would like more guidance from the EAC. Virginia Elections Commissioner, Edgardo Cortés said, "At a minimum Congress should empower and fund the EAC to expand their current voluntary voting system guidelines to include guidelines applicable to electronic poll books."[233] In addition, the EAC can provide request for proposal (RFP) templates to help states ensure that their election technology vendors are prioritizing cybersecurity, and the EAC could create training modules to assist states in providing cybersecurity education to election officials, IT staff, and poll workers.

Department of Homeland Security

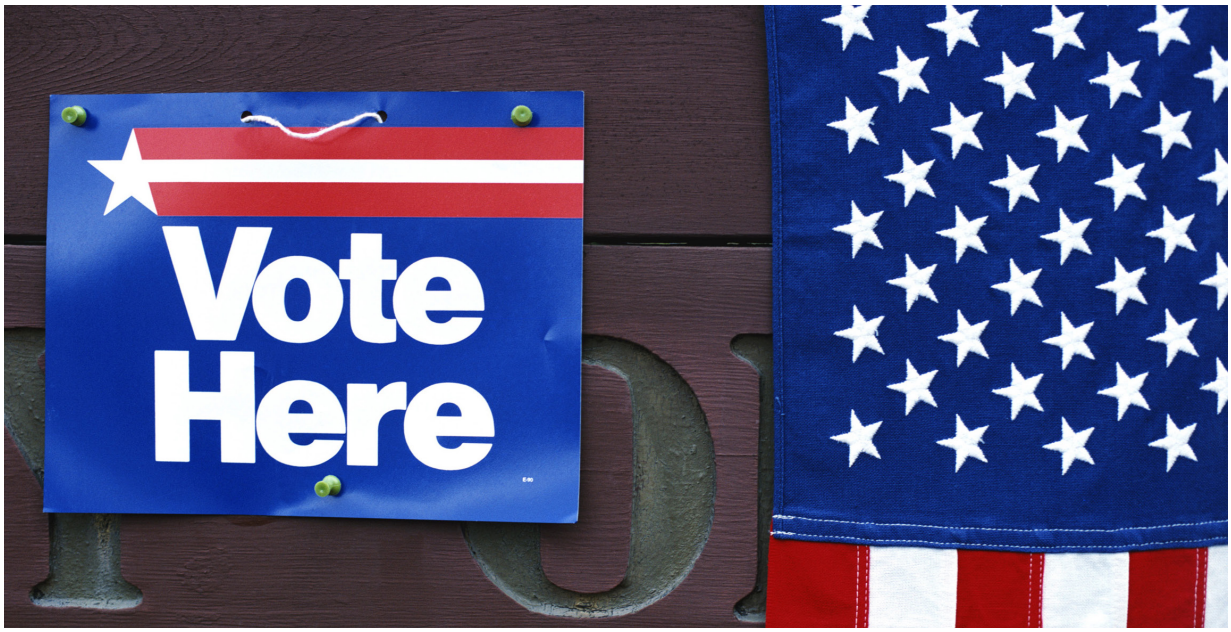
DHS has resources it can bring to bear on securing elections, but there are some roadblocks to overcome. As one DHS official noted before the

Senate Intelligence Committee in June, "Addressing cybersecurity challenges and helping our customers assess their cybersecurity risk is not new for DHS."[234] Through NPPD, DHS can provide election officials with cyber threat intelligence, vulnerability assessments, penetration testing, scanning of databases and operating systems, and other cybersecurity services at no cost. Through these services, state and local election officials can learn how to practice better cyber hygiene, make sure voting systems are operating securely and kept offline and carry out routine vulnerability assessments on voter registration databases. DHS can also help states carry out comprehensive risk assessments on a regular basis.

Some of the hurdles DHS experienced before and after the 2016 election are inherent in the challenge of standing up a new sector and learning to communicate with a new stakeholder community. As the DHS Assistant Secretary for Cybersecurity & Communications testified in June, "[H]istorically, DHS has not had active engagement directly with the state and local election community, so we're working on broadening and deepening those relationships, identifying requirements, and educating on our capabilities."

Representatives from the elections community readily acknowledge how unique, small, and close-knit their stakeholder group is – and many aspects of the environment they operate in do not apply in other critical infrastructure sectors. For instance, election officials operate on a strict timeline, and often cannot make updates to voter registration databases and other systems for some window of time prior to an election. In addition, officials are frustrated by the fact that they have to wait nine months to receive a service for which they are entitled 'priority access.'

Where DHS has rendered assistance, officials report that cyber hygiene scans and other services are valuable; however, because these services are voluntary, DHS' ultimate success depends on its ability to build trusted partnerships with state and local election officials. Elections are cyclical, and DHS needs adequate resources to carry out its election security activities without further depleting the goodwill it has in the elections community.



ELECTION VENDORS ARE UNREGULATED TARGETS

Many states utilize third party vendors to provide their election technology software and hardware. States utilize vendors to create and maintain the statewide voter registration database that they were required to create under HAVA, and they purchase voting machines and accompanying software from outside companies as well. Local election offices are unlikely to have any internal IT staff, so election vendors often end up providing IT support as well.[235] As demonstrated in the 2016 election, these vendors are a tempting target for hackers as breaching an election technology vendor has the potential to provide a hacker access to numerous election jurisdictions. Despite the risks associated with these third-party vendors, they are unregulated at the federal level.

A NSA document leaked to *The Intercept* highlights the vulnerability presented by election technology vendors.[236] *The Intercept* reports that Russia's plan in 2016 was to pose as an election vendor and email local election officials with the hope that the officials would open an attachment containing malware.[237] In order to execute this plan, Russian hackers sent spear-phishing emails to an election software vendor. The NSA report indicates that at least one employee account was compromised, though the targeted vendor, VR Systems, says that no employee accounts were compromised.[238] Russian hackers went on to pose as VR Systems employees and send over 100 emails to local government email addresses.

This was one of several tactics used by the Russians in their multifaceted campaign to sow doubt about the democratic process.[239] In addition to attempting to hack in state and local election systems, the Russians also conducted cyber espionage against the Democratic National Committee and key personnel in the Clinton campaign, and launched a propaganda campaign utilizing Facebook, Twitter and other social media to exacerbate divisions and undermine faith in democracy.[240] According to testimony before the House Permanent Select Committee on Intelligence in November, the propaganda was far-reaching –social media companies revealed that Russian agents spread Facebook posts that reached 126 million people, uploaded more than 1,000 videos to YouTube, and sent more than 131,000 tweets. If the attack against election vendors had been successful and the hackers were able to infect the computers of the local election officials, hackers may have been able to access state voter registration databases and alter or delete voter registration records. At the very least, this could have caused a great deal of chaos on election day. At worst, hackers could have deleted registration records of voters inclined to voter for a certain candidate thereby swaying the results of the election.

There is no federal law that governs what steps election vendors must take to safeguard their systems from attack. Instead, any obligations that vendors are subject to stem from the terms of their contracts with states and localities. The chief executives of VR Systems told the Task Force that their contracts did not have any specific requirements on: 1) what cybersecurity practices must be followed and 2) when state and local election officials needed to be notified in the event of a cyberattack.[241] Nevertheless, before they were targeted by the Russians, VR Systems did expend resources on cybersecurity. Once the company became aware of the suspicious activity, they notified the FBI and their clients. Since the election, the company has redoubled their efforts, enlisting a private security firm to help them harden their systems.[242] However, absent any regulation in this area, there is no way to know whether other third-party vendors would also have notified election officials and clients about a cyberattack. More importantly, instead of approaching election technology vulnerabilities as a national security issue, we are allowing companies to determine for themselves whether it is in their financial best interest to be concerned with cybersecurity.

According to a recent study put out by the Penn Wharton Public Policy Initiative, the election technology industry is dominated by three firms whose products cover approximately 92% of the total eligible voter population.[243] These firms are neither publicly nor independently held which limits the amount of publicly available information available about their operations.[244] Smaller companies routinely get bought out and merged with one of the three larger companies, and biggest tech companies, including Apple, Dell, IBM, HP, and Microsoft have chosen to stay out of the election technology business.[245] This may in part be because the sector generates approximately $300 million in annual revenue, a relatively modest amount when compared to the revenue of the largest technology companies. For example, Apple generates about $300 million in revenue every 12 hours.[246]

Currently, election technology vendors present serious security risks. The consolidation in the election technology industry means that "there is no meaningful competitive pressure from the suppliers to the vendors."[247] In other words, there is no incentive for election technology vendors to prioritize security. This problem is compounded by the lack of regulation in this area. These vendors are not required to make financial disclosures to the Securities and Exchange Commission. The executives are not required to disclose political contributions to the Federal Elections Commission. State and local contracts do not necessarily require vendors to notify election officials in the event of a cyberattack. Under current law, there is no way to ensure that vendors are doing everything possible to keep their systems secure.

The Task Force believes this must change. States and counties must hold vendors accountable and ensure that they are prioritizing election security. The EAC should provide RFP templates that include language on cybersecurity practices and incident notification.

States and localities should include such language in their RFPs, and seek to include security provisions in their existing contracts. Alternatively, the EAC could put forth a set of standards for election vendors to follow and then certify vendors who are following best practices, similar to the testing and certification program the Commission administers in the voting machine context.

Election Security is National Security

Russian interference in the 2016 Presidential election was a watershed moment in our democracy. By weaponizing the information we consume, eroding confidence in our political institutions, and pressure-testing the equipment we use to cast our ballots on Election Day, the Kremlin was able to use the democratic process as an attack vector. Securing this new and novel attack vector will require a novel approach.

After the 9/11 terrorist attacks, the nation had to confront the difficult reality that the attacks might have been prevented with better information sharing and more robust interagency collaboration. We struggled to balance the need to protect information while also empowering the right agencies to act in the face of threats. We had to overcome an initial reluctance to share turf with new partners and move past fears of reputational damage. It was nevertheless clear that the threat landscape had changed, and our security framework needed to change with it.

The threat landscape has once again shifted, exposing new cracks in our existing security framework and causing another set of turf wars. The Obama Administration worked proactively to assist state and local governments secure their election systems and, in January, declared election infrastructure a critical infrastructure subsector. Unfortunately, the Trump Administration's commitment to election security is less clear. The President continues to waffle on the Intelligence Community's conclusions regarding Russian efforts to meddle in the 2016 elections, re-opening questions about the validity of their assessment as recently as November 2017.[248] These actions indicate the Trump Administration is failing to take the threat to election infrastructure and democratic institutions seriously. Moreover, although the recently-released National Security Strategy refers to Russia's influence operations, it is unclear how the Administration plans to ensure the security of U.S. election infrastructure going forward.

Election Infrastructure is Critical Infrastructure

Federal law defines critical infrastructure as 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 thereof. For infrastructure designated critical, DHS offers priority access to cyber threat intelligence, incident response, technical assistance, and other products and services to help owners and operators harden their defenses.

It is hard to imagine a system failure that would inflict more damage than a foreign adversary infiltrating our voting systems to hijack our democratic process. However, the decision to designate a critical infrastructure sector or subsector ultimately falls to the Secretary of Homeland Security. This summer, former Secretary of Homeland Security John Kelly wavered on his earlier commitment to honor his predecessor's designation. Although Secretary Kirstjen Nielsen has said she will maintain the designation, she is not obligated to do so.

Defining election systems as critical infrastructure means these systems will, on a more formal and enduring basis, be a priority for DHS cybersecurity assistance. These services are an important force multiplier, especially at the state and local level, where resources are scarce.

Russia Will Continue its Efforts to Undermine Western Democracies, and Sophisticated, State-sponsored Actors Will Continue to Pursue Cyberattacks

As former Under Secretary for NPPD Suzanne Spaulding observed: "Russia is engaged in a long-term effort to undermine democracy both tactically to weaken the west and strategically to reduce liberal democracy's appeal not just in the United States but. . . around the world where Russia competes for influence and power."[249]

Russia has a long history of using cyberattacks and cyber-enabled disinformation campaigns to target political processes in other nations, adhering to a foreign policy built to leverage "the force of politics as opposed to the politics of force."[250] By carrying out advanced influence operations, Russia is able to "punch above their weight" by "provid[ing] their relatively weak economy and insecure political institutions with a strategic and tactical advantage to affect significant political outcomes abroad."[251] The advent of social media and data analytics have allowed Russia a new forum to alter the course of events by manipulating public opinion.[252]

The United States is also not Russia's only target. Russia orchestrated politically-motivated cyber campaigns in the Netherlands, France, Germany, Bulgaria, Estonia, Austria, and two Ukrainian presidential elections in 2004 and 2014, a decade apart.[253] Similar to the 2016 U.S. election, these efforts by Russian hackers were aimed at skewing the results, sowing discord, and undermining public faith in the media, government institutions and the democratic process itself. Russia has established a consistent pattern of conducting new and aggressive attacks on election infrastructure, particularly in the United States and Europe.[254] These efforts are part of Russia's larger strategy to undermine trust in our democracies, and are also likely part of a broader attempt to divide Europe from America, and to weaken both NATO and the European Union.[255] There is no evidence that Russia will forfeit the capabilities they have spent decades crafting and cease these efforts. Moreover, security experts are warning that Russia may turn to new frontiers like Mexico, which will elect more than 3,000 government officials in July 2018.[256]

In addition, other adversaries hostile to western democracies could seek to replicate its election interference campaign, many well-respected security experts have warned.[257] Possible nation-states that could exploit vulnerabilities in our elections also include North Korea, Iran, and China.[258] Any of these scenarios would be catastrophic – if only for the damage it would do to public confidence.

The federal government needs a better understanding of how Russian efforts to interfere in the 2016 Presidential election fit into its larger global agenda, and a strategy to protect our democratic institutions from all hostile actors going forward.

RECOMMENDATIONS

Federal Funds Should be Provided to Help States Replace Aging, Vulnerable Voting Machines with Paper Ballots

The most urgent need is to replace all DRE machines. There are two types of DRE machines in use: 1) paperless machines and 2) those equipped with a VVPAT. Both types of machines present significant security risks as the DRE systems store voting records in the machine's internal memory. Paperless systems make it impossible to practically detect whether there has been tampering with an election's results. Though the VVPAT systems purport to leave a paper audit trail by providing a receipt or printout of a voter's selections, the voter record that gets tabulated still lives in the machine's internal memory. This means that the printout the voter receives does not necessarily indicate whether the vote will be tabulated correctly. Thus, the auditability provided by the voter-verified receipt is of little value. Twenty-four states use DRE machines – fourteen use paperless DREs and an additional ten use VVPAT systems.[259]

There is widespread consensus that these machines need to be replaced, with emphasis on the need to replace paperless DREs, and that they should be replaced with paper ballots. A letter from over 100 computer science and cybersecurity experts was sent to every Member of Congress in June 2017 with recommendations on securing election systems. The first recommendation was to phase out paperless DRE machines.[260] If there was any remaining doubt, DefCon's voting village showed the country just how easy it is to breach paperless DRE machines.[261] In interviews with the Task Force, many election cybersecurity experts stated that VVPAT systems pose significant security risks and should be replaced as well.[262]

Of the voting systems in use today, experts agree that the most secure voting system is one where a voter marks a paper ballot, and the ballots are then counted by an optical scanner machine. Though optical scanner machines are not wholly immune from cyberattacks, a paper ballot filled out by a voter produces an auditable paper trail that can easily detect attacks.[263]

Jurisdictions must also be sure to comply with HAVA and ensure that disabled voters have access to voting systems that enable them to vote privately and independently. For example, some states use ballot-marking devices to ensure that their voting systems are accessible. A ballot-marking device is a tablet or laptop that does not have internet connectivity and is hardwired to an off-the-shelf printer and produces a paper ballot. In New Hampshire, these ballot-marking devices are being used along with software that has been tested by voters who cannot see or hear and by voters who cannot use their hands.[264] Such a device allows voters to cast their ballot privately and independently while also producing an auditable paper record.

Election administrators agree that they need to replace their aging voting machines, but many say they cannot act because they do not have the necessary funds. South Carolina is one of the five states that relies exclusively on paperless DREs, and a spokesman for the South Carolina Election Commission recently told the New York Times, "We're using the same equipment we've used since 2004. If $40 million dropped into our hands today, we'd have a paper ballot trail, too."[265] In a recent Politico survey, 21 of 33 respondents want the federal government to authorize funds for states to spend on replacing voting machines or otherwise strengthening election security.[266] In response to the letter sent out by the Task Force to

the chief election official in each state, four states (Minnesota, Nebraska, Illinois, and Pennsylvania) of the National Association of Secretaries of States expressed a desire for Congress to appropriate funds to help states replace aging voting equipment.[267]

The Brennan Center estimates that the cost to replace paperless DREs would be between $130 and $400 million. However, that figure does not include the additional cost associated with replacing VVPAT systems.

Congress has money available that they could use to help states replace their old machines. HAVA authorized $3 billion to meet the statute's requirements, and over $300 million remains to be appropriated.[268] Congress should act immediately to allow states to use this money.

States Should Conduct Risk-Limiting Post-Election Audits

While we can and should do everything possible to prevent an attack from taking place, the best way to determine with a high degree of certainty, whether an attack has taken place, is for states to conduct mandatory, routine, risk-limiting post-election audits. A statistically sound post-election audit would enable states to determine that the original vote count was substantially accurate. These audits are useful in detecting any incorrect election outcomes, whether they are caused by a cyberattack or something more mundane like a programming error. Moreover, conducting these audits as a matter of course increases public confidence in the election system.[269]

A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct.[270] The initial number of ballots is determined by a number of factors, including the margin of victory in the contest – the larger the margin of victory, the smaller the initial sample. If the audit finds strong evidence that the result was correct, the audit stops. However, if the initial sample is insufficient to confirm the election result, there will be a second round of hand-counting with a larger sample of ballots. This goes on until the auditor can determine with certainty that the election result was accurate. If the evidence never becomes strong enough to support that conclusion, a full hand count will be conducted.[271]

Because of the use of sophisticated statistical methods and the iterative process, risk-limiting audits provide an efficient and cost-effective way to verify election results. Professor Halderman estimates that the cost of running risk-limiting audits nationally for federal elections would be less than $20 million a year.[272]

According to Professor Halderman, currently, only two states, New Mexico and Colorado, "conduct audits that are robust enough to detect cyberattacks."[273] Rhode Island recently passed legislation providing for risk-limiting audits begin in 2018 and post-election risk-limiting audits in 2020.[274] Election security experts agree that all states should be routinely conducting these audits to detect any anomalies in election results and to increase the public's confidence in elections.[275]

Federal Funds Should be Provided to Help States Upgrade and Maintain IT Infrastructure, Including Voter Registration Databases

Russia's targeting of 21 states' voter registration systems, and the successful breach of the Illinois database, makes abundantly clear that our voter registration systems are vulnerable. Fortunately, the hackers' attempts to alter and delete records were blocked, but they had access to the Illinois voter files for almost three weeks before their activity was detected.[276] Russian hackers also came close to accessing a statewide voter registration database in Gila County, Arizona where an employee opened an infected email attachment that then installed malware on the employee's computer.[277] If any of these attempts had been successful, voting records could have been added, altered, or deleted, and Election Day would be filled with chaos. Just as significantly, such an attack would sow deep doubts about the integrity of our elections and American democracy. These close calls show that it is crucial that states act now to upgrade and secure their IT infrastructure.

The first steps to securing voter registration databases and other IT infrastructure is to replace outdated technology and hire the necessary IT support. In at least 41 states, databases are at least a decade old, and threats have evolved significantly since then.[278] The problem of an aging system is often compounded because many jurisdictions relying on older, less secure software and operating systems may also lack IT support. Election administration systems are often run on a different network than the rest of the state, and do not receive support from the office of the Chief Information Officer.[279] Many states report that they are unable to get the IT support they need, particularly at the local level.[280] Systems that are relying on antiquated software or operating systems should be modernized, and state and local election officials should have the IT support they need.

In addition, election administrators should follow cyber-security best practices, including regular backups. Several officials that spoke to the Task Force indicated that it would be useful for DHS or the EAC to provide guidance documents that outline cybersecurity best practices.[281]

Many states are already implementing these recommendations, and even more have started in the wake of the 2016 election.[282] States are hiring new technology support staff and upgrading their voting systems wherever possible. However, states need money. After conducting a survey of state election officials, where 21 out of 33 states indicated that they need help funding security improvements, *Politico* reported, "States need money to upgrade digital voter registration systems that alleged Russian hackers probed and infiltrated in 2016. They need money to provide cybersecurity training to local county officials… And they need money to adopt new post-election audit procedures that can detect vote tampering."[283]

We cannot ask our state and local election officials to take on a state actor like Russia alone. Although states and counties are largely responsible for elections, Congress has a role to play in helping states fund the purchase of newer, more secure election systems, and requiring such systems adhere to baseline cybersecurity standards. Congress should direct DHS and EAC to work together to define security standards for election equipment and appropriate the funding necessary to help state and local governments replace outdated voting systems.

It is important to note that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials. Congress must establish a mechanism to provide ongoing support to state and local governments. One way to do that would be to reimburse states for part of the cost associated with administering federal elections by providing a flat rate per active registered voter, as many states do when counties are responsible for administering state ballot questions.

In addition, Congress should appropriate funds for innovation grants so that new technology can be developed to respond to the evolving threat landscape.

Election Technology Vendors Must Secure Their Voting Systems

Many states purchase their voting systems from a third-party vendor. Those vendors have little financial incentive to prioritize election security, and there no regulations requiring them to use cybersecurity best practices. The Task Force recommends that the EAC provide RFP templates that would require vendors to: 1) secure their systems, and 2) notify state and local officials in the case of a cyberattack. States and localities should use this language in all future contracts, and seek to incorporate these requirements into their existing contracts. In addition, election technology vendors should be required to inform EAC and DHS officials in the event of a cyberattack.

The Federal Government Should Develop a National Strategy to Counter Efforts to Undermine Democratic Institutions

The goals of Russian efforts to meddle in the 2016 presidential election were not limited to promoting one candidate or damaging another; they were an attempt to undermine confidence in democratic institutions and sow doubt in liberal democracies. As a former Under Secretary for NPPD warned, "We need to broaden our focus to the ways these measures undermine other fundamental pillars of democracy, including the press and our judicial system."[284]

Past attacks of this magnitude have served as a catalyst for major strategic changes and a re-orientation of federal policy. Our starting point is clear – we need a strong, consistent rebuke from the White House. Next, we need the President to acknowledge that we need a "9/11-style" Commission to help identify the various ways in which the Russians are seeking to undermine democracy and develop a plan to confront them. After the terrorist attacks of September 11, 2001, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) undertook this effort to understand the full impact of this tragic event and resolve the gaps in our security framework.

The Intelligence Community Should Conduct Pre-Election Threat Assessments Well in Advance of Federal Elections

It is clear that efforts to disrupt the administration of elections are going to continue. To empower state and local governments to secure their election systems and to inform federal efforts to support them, there must be a current, complete understanding of the threat landscape. At the same time, state and local election officials must know of relevant intelligence related to efforts to target elections with an adequate amount of time to assess vulnerabilities within their systems and networks and address them. Moreover, any threat assessment must be conducted sufficiently in advance of the election to avoid the perception of political motivation.

Accordingly, the Intelligence Community should complete and provide to Congress and state and local election officials an assessment of the full scope of threats to election infrastructure 180 days prior to federal election, together with recommendations provided by DHS and EAC to address them. The assessments should be unclassified, with the option of adding a classified annex, as necessary. To ensure that state and local election officials have access to all information necessary to protect their election infrastructure, the Department of Homeland Security should expedite the clearance process for relevant officials and/or provide one-day "read-in" clearances.

DHS Should Maintain the Designation of Election Infrastructure as a Critical Infrastructure Subsector

Defining election systems as critical infrastructure means election infrastructure will, on a more formal and enduring basis, be a priority for DHS cybersecurity services. These services are an important force multiplier, especially at the state and local level, where resources are scarce. We have a rare window of opportunity to promote the widespread adoption of common-sense security measures that protect the integrity of the ballot box. This is not the time to diminish federal efforts or shut down important lines of dialogue between DHS and election administrators.

Empower Federal Agencies to be Effective Partners in Pushing out Nationwide Security Reforms

With midterm elections less than a year away, election officials cannot afford to wait 9 months for valuable cybersecurity services like Risk and Vulnerability Assessments. At the same time, Congress should not put DHS in the position of delivering election assistance at the expense of its other critical infrastructure customers. DHS must conduct a comprehensive assessment of the funding, resources, and personnel it needs to deliver the services state and local elections officials request to secure their election

infrastructure, and make a request to Congress. In turn, Congress must act and give DHS the resources it needs to meet its obligations to state and local election officials, as well as all critical infrastructure owners and operators.

Similarly, Congress should fund EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.

Establish Clear and Effective Channels for Sharing Threat and Intelligence Information with Election Officials

Effective information sharing is critical to addressing the decentralized threat that our nation faces in terms of securing our elections. We have seen how information sharing failures can cause catastrophic events prior to the 2016 elections. The 9/11 terrorist attacks exposed serious gaps in information sharing within the federal government and state and local law enforcement partners. It is imperative that election officials have access to the most timely and high-level security information. Chief election officials in each state should have expedited access to security clearances. DHS needs a formalized process to provide real-time appropriate threat information to state and local election officials to improve information flow and help prevent intrusions in our election infrastructure. Additionally, DHS has experience helping non-traditional preparedness and response stakeholders partner together to address evolving threats. The Department should leverage that experience, and provide states models for effective information sharing protocols related to election infrastructure. Finally entities involved in administering elections, as well as political organizations, should consider forming an information sharing and analysis organization to share data on cyber threats.

States Should Prioritize Cybersecurity Training

"Training the trainers" is a crucial component in securing elections. The events of 2016 demonstrate that human error is a significant vulnerability as it leaves systems open to spear-phishing and other forms of cyberattack. Election officials have told the Task Force that building the capacity of local election officials and IT staff remains a challenge.[285] Secretary Nellie Gorbea stated, "Our public sector employees and system at the state, county, and municipal level are ill-prepared to handle the looming threat of cyberattacks."[286] States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation.

It costs money for states to produce training materials, and takes staff time to implement statewide training programs. The federal government should provide training support either through the EAC or by providing funding to states to assist with their training programs. With additional resources, the EAC could produce templates for states to use, or could assist states in reviewing training materials created in-state. In addition, the EAC is currently working with Harvard's Belfer Center to develop a tabletop training which could be useful to states looking to incorporate cybersecurity education into their trainings.[287] In the meantime, states with resources to do so should follow the lead of Secretaries of State who are taking action to raise awareness about how to keep election infrastructure secure. Rhode Island Secretary of State Nellie Gorbea, for example, convened a meeting of federal, state, and local officials, including more than one hundred of Rhode Island's municipal election officials and IT staff, for a summit on elections cybersecurity.[288]

CONCLUSION

The attacks in 2016 preview what is yet to come. In March 2017, then-FBI Director James Comey testified before the House Permanent Select Committee on Intelligence that: "[T]hey'll be back. They'll be back in 2020. They may be back in 2018."[289] Just days before the 2017 elections, Bob Kolasky, the acting Deputy Undersecretary of the National Protection and Programs Directorate at the Department of Homeland Security said, "We saw in 2016 that Russia had an intent to be involved in our elections and some capability to be active or to attempt to be active in scanning election systems. We have not seen any evidence that intent or capability has changed."[290] The threat remains, and Congress must act.

When a sovereign nation attempts to meddle in our elections, it is an attack on our country. We cannot leave states to defend against the sophisticated cyber tactics of state actors like Russia on their own. Michael Chertoff, former Secretary of Homeland Security wrote in *The Wall Street Journal*, "In an age of unprecedented cyber risks, these dangers aren't surprising. But lawmakers and election officials' lackadaisical response is both staggering and distressing… This is a matter of national security, and Congress should treat it as such." We urge Congress to act in a bipartisan fashion and take action – to provide the necessary funding, to take seriously the recommendations of this Task Force, and to recognize that election security is national security.

TASK FORCE ACTIVITY APPENDIX

PUBLIC FORUMS

Securing America's Elections: Understanding the Threat
Witnesses: The Honorable Jeh Johnson, *former Secretary of Homeland Security*, and the Honorable Suzanne Spaulding, *former Department of Homeland Security Under Secretary for the National Protection and Programs Directorate.*

Securing America's Elections: Preparing for 2018 and Beyond
Witnesses: The Honorable Nellie Gorbea, *Rhode Island Secretary of State*, Mr. Edgardo Cortés, *Virginia Department of Elections Commissioner*, and Mr. Thomas Hicks, *Election Assistance Commission Commissioner & Vice-Chair*.

OFF-SITE MEMBER AND STAFF BRIEFINGS

Cyber Vulnerabilities in U.S. Voting Infrastructure, presented by *DEFCON Hackers and National Security Leaders at The Atlantic Council*

Election Assistance Commission Public Meeting

National Security Imperative of Addressing Foreign Cyber Interferences in U.S. Elections, *Brookings Institute*

Solutions to Secure America's Elections, *Center for American Progress*

ON-SITE MEMBER AND STAFF MEETINGS AND BRIEFINGS

Access Democracy

Mr. Jake Braun, *Cambridge Global Advisors*

Dr. Ben Buchanan, *Harvard University*

Brennan Center for Justice

Dr. Judd Choate, *National Association of State Election Directors President*

Department of Homeland Security

Mr. Jim Dickson, *National Council on Independent Living Voting Rights Task Force*

Election Assistance Commission

Dr. Edward W. Felten, *Princeton University*

Free and Fair Election Technologies

Dr. Juan Gilbert, *University of Florida*

Dr. J. Alex Halderman, *Michigan State University*

Dr. John Koza, *Michigan State University*

National Association of Secretaries of State

National Association of State Chief Information Officers

National Governors Association

Open Source Election Technology Institute

Dr. John Savage, *Brown University*

Ms. Marian Schneider, *former Special Advisor to the Governor of Pennsylvania on Election Policy*

The Honorable Steve Simon, *Minnesota Secretary of State*

Verified Voting

VR Systems

Mr. Luther Weeks, *State Auditability Working Group*

ENDNOTES

1 Official Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

2 Office of the Director of National Intelligence Declassified Report, "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution," at iii (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

3 Joe Uchill, "DHS tells 21 states they were Russia hacking targets before 2016 election," The Hill (Sep. 22, 2017), http://thehill.com/policy/cybersecurity/351981-dhs-notifies-21-states-of-they-were-targets-russian-hacking.

4 Dustin Volz and Jim Finkle, "Voter Registration Databases in Arizona and Illinois Were Breached, FBI Says," TIME (Aug. 29, 2016), http://time.com/4471042/fbi-voter-database-breach-arizona-illinois/.

5 Open Hearing on Russian Active Measures Investigation before the House Permanent Select Committee on Intelligence, 115th Cong. (Mar. 20, 2017), (statement of James Comey, Director, Federal Bureau of Investigation), available at http://www.cq.com/doc/congressionaltranscripts-5065176?1.

6 Reid Wilson, Election Officials Race to Combat Cyberattacks, The Hill (Nov. 8, 2017) http://thehill.com/homenews/campaign/359243-election-officials-race-to-combat-cyberattacks.

7 Cory Bennett et al., Cash-Strapped States Brace for Russian Hacking Fight, POLITICO (Sept. 3, 2017) http://www.politico.com/story/2017/09/03/election-hackers-russia-cyber-attack-voting-242266.

8 Governor Rick Scott's 2017-2018 Budget, (last visited, Oct. 18, 2017) http://fightingforfloridasfuturebudget.com/web%20forms/Budget/BudgetService.aspx?rid1=327714&rid2=298915&ai=45000000&title=STATE.; Jackie Borchardt, Ohio Gov. John Kasich Vetoes Medicaid Freeze, Signs State Budget Bill, Cleveland.com (Jul. 10, 2017) http://www.cleveland.com/metro/index.ssf/2017/06/ohio_gov_john_kasich_signs_sta.html; Veto Message in Brief, Sept. 20, 2017, p. 13. https://walker.wi.gov/sites/default/files/09.20.17%20Veto%20Message%20in%20Brief.pdf.

9 Bennett, supra n. 7.

10 Letter from Connie Lawson, President, National Association of Secretaries of State, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 3, 2017) (on file with author).

11 Burris, A. L., Fischer, E.A. (2016) The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election (CRS Report No. RS20898).

12 Risk-Limiting Audits Working Group, Risk-Limiting Post-Election Audits: Why and How, 5, (Jennie Bretschneider et al. eds., 1.1 version, 2012) https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

13 Office of the Director of National Intelligence Declassified Report, "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution," at iii.

14 Id.

15 Id. See also Open Hearing on Russian Interference in European Elections Senate Select Committee on Intelligence, 115th Cong. (Jun. 28, 2017), (statement of Ambassador (ret.) Nicholas Burns), available at https://www.intelligence.senate.gov/sites/default/files/documents/sfr-nburns-062817b.pdf.

16 Open Hearing on Russian Interference in European Elections Senate Select Committee on Intelligence, 115th Cong. (Jun. 28, 2017), (statement of Ambassador (ret.) Nicholas Burns), available at https://www.intelligence.senate.gov/sites/default/files/documents/sfr-nburns-062817b.pdf. See also Jason Le Miere, "Russia Election Hacking: Countries Where the Kremlin Has Allegedly Sought to Sway Votes," Newsweek (May 9, 2017), available at http://www.newsweek.com/russia-election-hacking-france-us-606314; James Ludes and Mark Jacobson, "Shatter the House of Mirrors: A Conference Report on Russian Influence Operations," Pell Center, (Sept. 26, 2017), available at http://pellcenter.org/wp-content/uploads/2017/09/Shatter-the-House-of-Mirrors-FINAL-WEB.pdf; Heather Conley and Ruslan Stefanov, "The Kremlin Playbook," CSIS (Oct. 13, 2016), available at https://www.csis.org/analysis/welcome-kremlin-playbook; Alina Polyakova et al., "The Kremlin's Trojan Horses," The Atlantic Council, (Nov. 15, 2016), available at http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf; Christopher Paul and Miriam Matthews, "The Russian Firehose of Propaganda Model," RAND, (Dec. 13, 2016), available at https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf; and Minority Staff Report of the House Committee on Science, Space, and Technology Subcommittee on Oversight, "Old Tactics, New Tools: A Review of Russia's Soft Cyber Influence Operations," (Nov. 2017), available at https://democrats-science.house.gov/sites/democrats.science.house.gov/files/documents/Russian%20Soft%20Cyber%20Influence%20Operations%20-%20Minority%20Staff%20Report%20-%20November%202017_0.pdf.

17 Office of the Director of National Intelligence Declassified Report, "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution," at iii.

18 Id.

19 Id.

20 Some reports suggest that voting systems in as many as 39 states were infiltrated by Russian hackers. Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg (Jun. 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

21 Id.

22 Testimony of Jeh Johnson, former U.S. Secretary of Homeland Security, and Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-markups/hearings/task-force-election-security-securing-americas-elections-understanding. See also Morgan Chalfant, "Obama DHS officials pitch election cybersecurity fixes to Congress," The Hill (Sep. 28, 2017), http://thehill.com/policy/cybersecurity/352919-obama-era-dhs-officials-pitch-election-cybersecurity-fixes-to-congress?utm_source=&utm_medium=email&utm_campaign=11067.

23 Testimony of James Comey, Federal Bureau of Investigations, before the House Permanent Select Committee on Intelligence hearing entitled Open Hearing on Russian Active Measures Investigation (Mar. 20, 2017), transcript available at https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.a3209228adef.

24 Testimony of Jeh Johnson, former U.S. Secretary of Homeland Security, and Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-markups/hearings/task-force-election-security-securing-americas-elections-understanding. See also Morgan Chalfant, "Obama DHS officials pitch election cybersecurity fixes to Congress," The Hill (Sep. 28, 2017), http://thehill.com/policy/cybersecurity/352919-obama-era-dhs-officials-pitch-election-cybersecurity-fixes-to-congress?utm_source=&utm_medium=email&utm_campaign=11067.

25 Id. See also Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference," Brennan Center (Jun. 29, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference; Michael O'Hanlon, "Cyber Threats and How the United States Should Prepare," The Brookings Institution (Jun. 14, 2017), available at https://www.brookings.edu/blog/order-from-chaos/2017/06/14/cyber-threats-and-how-the-united-states-should-prepare/; The Brookings Institution, "The National Security Imperative of Addressing Foreign Cyber Interference in U.S. Elections," The Brookings Institution (Sept. 8, 2017), available at https://www.brookings.edu/wp-content/uploads/2017/09/20170908_election_security_transcript.pdf; and Ian Livingston, "Securing the Vote Is Critical to Preserving American Democracy," The Brookings Institution (Sept. 21, 2017), available at https://www.brookings.edu/blog/order-from-chaos/2017/09/21/securing-the-vote-is-critical-to-preserving-american-democracy/. See also Reid Standish, "American Elections Remain Unprotected," The Atlantic, (Dec. 28, 2017), available at https://www.theatlantic.com/international/archive/2017/12/russia-disinformation-election-trump-putin-hack-cyber-europe/549260/; Michael Morell and Mike Rogers, "Russia never stopped its cyberattacks on the United States," The Washington Post, (Dec. 25, 2017), available at https://www.washingtonpost.com/opinions/russia-never-stopped-its-cyberattacks-on-the-united-states/2017/12/25/83076f2e-e676-11e7-a65d-1ac0fd7f097e_story.html?utm_term=.802d6d23a2f5; Tom Donilon, "Russia will be back. Here's how to hack-proof the next election," The Washington Post (Jul. 14, 2017), available at https://www.washingtonpost.com/opinions/russia-will-be-back-heres-how-to-hack-proof-the-next-election/2017/07/14/f085e870-67d5-11e7-a1d7-9a32c91c6f40_story.html?utm_term=.d14edd4000a9; "Russia Election Hacking: Countries Where the Kremlin Has Allegedly Sought to Sway Votes," Newsweek (May 9, 2017), available at http://www.newsweek.com/russia-election-hacking-france-us-606314; Elizabeth Weise, "After Russian Election Hack, U.S. Security Advisers Form Group to Make 2020 Race Unhackable," USA Today, (Oct. 10, 2017), available at https://www.usatoday.com/story/tech/news/2017/10/10/after-russian-election-hack-u-s-security-advisers-form-group-make-2020-race-unhackable/747403001/; Robby Mook, "Keep the Hackers Out of Our Elections," CNN (Aug., 2017), available at http://www.cnn.com/2017/08/24/opinions/keep-hackers-out-of-our-elections-opinion-mook/index.html; Matt Rhoades, "Every Campaign Is Now A Cyberwar Target," New York Post (Aug. 13, 2017), available at http://nypost.com/2017/08/13/every-campaign-is-now-a-cyberwar-target/.

26 Edward-Isaac Dovere, "Hacker Study: Russia Could Get into U.S. Voting Machines," Politico (Oct. 9, 2017), available at https://www.politico.com/story/2017/10/09/russia-voting-machines-hacking-243603. See also Ian Livingston, "Securing the Vote Is Critical to Preserving American Democracy," The Brookings Institution, (Sept. 21, 2017), available at https://www.brookings.edu/blog/order-from-chaos/2017/09/21/securing-the-vote-is-critical-to-preserving-american-democracy/. See also Rachel Ansley, "Russian Hacking: We Must Secure Our Voting Machines Right Now," Newsweek (Oct. 13, 2017), available at http://www.newsweek.com/russian-hacking-we-must-secure-our-voting-machines-right-now-684392; Matt Blaze, Jake Braun, and Harri Hursti et al., "DEFCON 25 Voting Machine Hacking Village," DEFCON Communications, Sept. 2017, available at https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf; and Harvard Kennedy School Belfer Center, "Belfer Center Launches Defending Digital Democracy Project to Fight Cyber Attacks and Protect Integrity of Elections," (Oct. 10, 2017), available at https://www.hks.harvard.edu/announcements/belfer-center-launches-defending-digital-democracy-project.

27 Ju-min Park and James Pearson, "Exclusive: North Korea's Unit 180, the Cyber Warfare Cell That Worries the West," Reuters (May 20, 2017), available at http://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020.

28 Id.

29 Id.

30 Testimony of General Curtis M. Scaparrotti, then-Commander U.S.-ROK Combined Forces Command, before the House Committee on Armed Services, Hearing on the NDAA, (Apr. 2, 2017), available at https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87862/html/CHRG-113hhrg87862.htm.

31 Timothy Phelps and Brian Bennett, "FBI Head Details Evidence That North Korea Was Behind Sony Hack," Los Angeles Times (Jan. 7, 2015), available at http://www.latimes.com/nation/la-na-comey-sony-north-korea-20150107-story.html.

32 Id.

33 Ju-min Park and James Pearson, supra n. 27.

34 Emma Chanlett-Avery, et al. "North Korean Cyber Capabilities: In Brief," Congressional Research Service (Aug. 3, 2017), available at https://fas.org/sgp/crs/row/R44912.pdf. See also Russell Goldman, "What We Know and Don't Know About the International Cyberattack," New York Times, (May 12, 2017), available at https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

35 Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Work to North Korea," Washington Post (Jun. 14, 2017), available at https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.95006ea82f53.

36 Thomas Bossert, "It's Official: North Korea is behind WannaCry," Wall Street Journal (Dec. 18, 2017), available at https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537. A recording of the December 19 briefing by President Donald Trump's homeland security adviser, Tom Bossert, is available at https://www.c-span.org/video/?438777-1/homeland-security-officials-blame-north-korea-wannacry-malware-attack.

37 Joseph Menn, "Symantec Says "Highly Likely' North Korea Group Behind Ransomware Attacks," Reuters (May 23, 2017), available at https://www.reuters.com/article/us-cyber-attack-northkorea/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks-idUSKBN18I2SH.

38 Emma Chanlett-Avery, et al, supra n. 34.

39 Joseph Menn, supra n. 37.

40 Jonathan Spicer and Joseph Menn, "U.S. May Accuse North Korea in Bangladesh Cyber Heist: WSJ," Reuters (Mar. 22, 2017), available at http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3. See also Council on Foreign Relations, "Cyber Operations Tracker," CFR, https://www.cfr.org/interactive/cyber-operations?utm_source=&utm_medium=email&utm_campaign=11915.

41 Jonathan Spicer and Joseph Menn, supra n. 40.

42 Ju-min Park and James Pearson, supra n. 27.

43 Eric O'Neill, "Nuclear War Isn't North Korea's Only Threat," CNN (Sept. 25, 2017), available at http://www.cnn.com/2017/09/23/opinions/north-korea-cyberattack-oneill-opinion/index.html.

44 "Russian firm provides new internet connection to North Korea," Reuters (Oct. 2, 2017), available at https://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2.

45 Testimony of Frank Cilluffo, Director of GWU's Homeland Security Policy Institute, House Committee on Homeland Security, 112th Cong. (Apr. 26, 2012) available at https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm.

46 Testimony of Frank Cilluffo, Director of GWU's Homeland Security Policy Institute, House Committee on Homeland Security, 112th Cong. (Apr. 26, 2012) available at https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm.

47 Center for Strategic & International Studies, "Significant Cyber Incidents," CSIS, https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity.

48 Eric Auchard, "Once 'Kittens' in Cyber Spy World, Iran Gains Prowess: Security Experts," Reuters (Sept. 20, 2017), available at http://www.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUSKCN1BV1VA?il=0

49 Id.

50 Id.

51 Kate Brannen, "Abandoning Iranian nuclear deal could lead to a wave of cyberattacks," Just Security, (Oct. 2, 2017), https://www.justsecurity.org/45549/abandoning-iranian-nuclear-deal-lead-wave-cyberattacks.

52 Siobhan Gorman and Danny Yadron, "Banks Seek U.S. Help on Iran Cyberattacks," The Wall Street Journal, (January 16, 2013), available at https://www.wsj.com/articles/SB10001424127887324734904578244302923178548.

53 Kate Brannen, supra n. 51.

54 Id.

55 Id.

56 Id.

57 Thomas Fox-Brewster, "Iranian Hackers Targeted Deloitte Via A Seriously Convincing Facebook Fake" In Homeland Security, (Oct. 5, 2017), http://inhomelandsecurity.com/iranian-hackers-targeted-deloitte-via-a-seriously-convincing-facebook-fake/?utm_source=IHS&utm_medium=newsletter&utm_content=iranian-hackers-targeted-deloitte-via-a-seriously-convincing-facebook-fake&utm_campaign=20171005IHS.

58 Kate Brannen, supra n. 51. See also Thomas Fox-Brewster, supra n. 57.

59 The Brookings Institution, "The National Security Imperative of Addressing Foreign Cyber Interference in U.S. Elections," The Brookings Institution (Sept. 8, 2017), available at https://

www.brookings.edu/wp-content/uploads/2017/09/20170908_election_security_transcript.pdf.

60 Thomas Fox-Brewster, supra n. 57.

61 Testimony of Frank Cilluffo, Director of GWU's Homeland Security Policy Institute, House Committee on Homeland Security, 114th Cong. (Feb. 25, 2016) available at https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg21527/html/CHRG-114hhrg21527.htm.

62 Center for Strategic & International Studies, "Significant Cyber Incidents," CSIS, https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity. *Note:* Although the United States has not formally attributed the hack to China, then-Director of National Intelligence James Clapper identified China as the leading suspect in June 2015 (see David Welna, "In Data Breach, Reluctance to Point the Finger at China," National Public Radio, Jul. 2, 2015). Moreover, a Chinese national was arrested in Los Angeles in August 2017 on charges he used a rare type of computer malware to access sensitive U.S. records from the Office of Personnel Management. See http://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.4cf2b6bdd4f7. For more on the OPM hacks unrelated to attribution, please see Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," Press Release (Jun. 4, 2015) and Office of Personnel Management, "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," Press Release (Jul. 9, 2015.) See also Council on Foreign Relations, "Cyber Operations Tracker," CFR, https://www.cfr.org/interactive/cyber-operations?utm_source=&utm_medium=email&utm_campaign=11915.

63 Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Press Release (May 19, 2014), available at https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

64 Center for Strategic & International Studies, "Significant Cyber Incidents," CSIS, available at https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity.

65 Council on Foreign Relations, "Cyber Operations Tracker," CFR, available at https://www.cfr.org/interactive/cyber-operations?utm_source=&utm_medium=email&utm_campaign=11915.

66 Testimony of Jennifer Kolde, Lead Technical Director, FireEye Threat Intelligence, House Committee on Homeland Security, 114th Cong. (Feb. 25, 2016) available at https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg21527/html/CHRG-114hhrg21527.htm.

67 Tobias Feakin, "Enter the Cyber Dragon," Australian Strategic Policy Institute (June 2013), available at https://www.files.ethz.ch/isn/165376/10_42_31_AM_SR50_chinese_cyber.pdf.

68 Homeland Security Act of 2002, §201 et seq, Pub. L. 107-296 (Nov. 25, 2002) (6 U.S.C. §121 et seq); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), §1016(e), Pub. L. 107-56 (Oct. 26, 2001) (42 U.S.C. §5195c) (defining critical infrastructure); White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (2013); Exec. Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing, 3 C.F.R. 271 (2015).

69 §201(d), P.L. 107-296 (6 U.S.C. §121(d)).

70 U.S. Election Assistance Commission, Voluntary Voting Systems Guidelines, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/ (last visited on Oct. 16, 2017).

71 U.S. Election Assistance Commission, Frequently Asked Questions, https://www.eac.gov/voting-equipment/frequently-asked-questions/ (last visited on Oct. 16, 2017).

72 Voting System Standards, Testing and Certification, National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx (June 8, 2017).

73 U.S. Election Assistance Commission, EAC Launches Tech Time Election Video Series, https://www.eac.gov/assets/1/28/EAC.Tech.Time.Videos.8.1.16.pdf (Aug. 1, 2016).

74 U.S. Election Assistance Commission, Managing Election Technology, https://www.eac.gov/voting-equipment/managing-election-technology/ (last visited on Oct. 16, 2017).

75 U.S. Election Assistance Commission, As Election Threats Persist, Chairman Masterson Affirms EAC Remains Poised to Support State and Local Response, https://www.eac.gov/news/2017/03/20/03/20/2017/ (Mar. 20, 2017).

76 Thomas Hicks, Commissioner and Vice-Chair of the Elections Assistance Commission, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct 24, 2017.

77 Id.

78 Nellie Gorbea, Secretary of State, State of Rhode Island, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct 24, 2017.

79 Verified Voting, House Rejects GOP Bill to Terminate Election Assistance Commission (Jun 23, 2011) https://thevotingnews.com/house-rejects-gop-bill-to-terminate-election-assistance-commission-the-hill/.

80 Burris, A. L., Fischer, E.A. (2016) The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election (CRS Report No. RS20898).

81 Oversight of the Federal Bureau of Investigation: Hearing Before Senate Committee On the Judiciary, 115th Congress (2017) (statement of James Comey, Director, FBI).

82 Election Assistance Commission, Elections – Critical Infrastructure, https://www.eac.gov/election-officials/elections-critical-infrastructure/ (last visited, Nov. 6, 2017).

83 EAC Reauthorization Act of 2017, H.R. 794, 115th Cong. (2017).

84 Message to the Congress of the United States from

President George W. Bush, proposal for The Department of Homeland Security (Jun. 18, 2002), https://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020618-5.html and https://www.dhs.gov/sites/default/files/publications/book_0.pdf.

85 See House Committee on Homeland Security, Report on the Homeland Security Act of 2002, 107th Congress, H. Report 107-609, at 63-7 (2002). The Report accompanying the Homeland Security Act of 2002 observed, "The changing nature of the threats facing the United States requires a new government structure to protect against invisible enemies that can strike with a wide variety of weapons" and "[a] single, unified homeland security structure will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future all the while protecting the freedom and liberty upon which this nation was founded." Id at 67. Related to emerging cyber threats against critical infrastructure, the Report predicted that "[i]n addition to physical destruction, terrorists may also seek to develop powerful forms of cyber attack against our critical infrastructures" and that "[w]hile there has been no 'electronic Pearl Harbor,' attacks of this nature will become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets, and the technologies required to attack them." Id. at 65-6. See also, U.S. National Commission on Terrorist Attacks upon the United States. 9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications, by Thomas H. Kean and Lee Hamilton, Washington, D.C. (2004) (citing inadequate information sharing and collaboration among the intelligence failures that led to the events of September 11, 2001), https://www.9-11commission.gov/report/911Report.pdf.

86 The full list of critical infrastructure sectors can be found in PPD-21: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems. Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

87 See, e.g., "Panetta Warns of Dire Threat of Cyberattack on U.S.," The New York Times (Oct. 11, 2012), available at http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

88 See generally, Chris Jaikaran, Cong. Research Serv., IF10683, DHS's Cybersecurity Mission – An Overview (Jun. 26, 2017).

89 See, e.g., "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," The New York Times (Dec. 13, 2016), available at https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

90 See generally, "Critical Infrastructure Resources," U.S. Department of Homeland Security, available at https://www.dhs.gov/critical-infrastructure-resources.

91 Id.

92 United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (Jul. 22, 2015), available at http://undocs.org/A/70/174.

93 Id.

94 U.S. Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

95 Critical Infrastructure Information Act of 2002, Pub. L. 107-296, §211 et seq (Nov 25, 2002) (6 U.S.C. §131 et seq). See also, Freedom of Information Act, Pub. L. 89-487, §3 (5 U.S.C. §552).

96 National Cybersecurity Protection Act of 2014, Pub. L. 113-282 (Dec. 18, 2014); Cybersecurity Act of 2015, Div. N. Consolidated Appropriations Act of 2016, Pub. L. 114-113 (Dec. 18, 2015).

97 Presidential Decision Directive/PPD-63, Protecting America's Critical Infrastructures (May 22, 1998) (introducing the ISAC model and calling on each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities).

98 See "Cybersecurity Information Sharing: Information Sharing and Analysis Centers (ISACs)," U.S. Department of Homeland Security, available at https://www.dhs.gov/topic/cybersecurity-information-sharing.

99 DHS does exercise limited regulatory authority over certain critical infrastructure sectors, see e.g., the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Pub. L. 113-254 (Dec. 18, 2014) (authorizing DHS to regulate high risk chemical facilities against the threat of terrorist attack).

100 Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 13, 2013).

101 Testimony of Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Select Committee on Intelligence, U.S. Senate (June 21, 2017), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF.

102 Testimony of Jeh Johnson, former U.S. Secretary of Homeland Security, and Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-markups/hearings/task-force-election-security-securing-americas-elections-understanding. See also Testimony of Jeanette Manfra, before the Select Committee on Intelligence, U.S. Senate (June 21, 2017), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF.

103 Letter from the Hon. Bennie G. Thompson, Ranking Member of the Committee on Homeland Security, U.S. House of Representatives to U.S. Secretary of Homeland Security Jeh Johnson, Department of Homeland Security (Aug. 8, 2016) (on file with Committee staff).

104 Id.

105 Id.

106 See, e.g., "U.S. Seeks to Protect Voting System From Cyberattacks," New York Times (Aug. 3, 2016), available at https://www.nytimes.com/2016/08/04/us/politics/us-seeks-to-protect-voting-system-against-cyberattacks.html?_r=1.

107 Readout of U.S. Department of Homeland Security Secretary Jeh Johnson's Call with State Election Officials on Cybersecurity, U.S. Department of Homeland Security (Aug. 15, 2016), available at https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity. On August 31, 2016, NASS named four Secretaries of State to serve on the panel: Connecticut State Secretary Denise Merill, Indiana State Secretary Connie Lawson, who also serves as the NASS President of and NASS Elections Committee Co-Chairs Alex Padilla (California) and Brian Kemp (Georgia). See Press Release from the National Association of Secretaries of States, NASS Appoints Secretaries of State to Federal Election Infrastructure Cybersecurity Working Group (Aug. 31, 2016), available at http://www.nass.org/node/238.

108 See, e.g., "DHS's New Election Cybersecurity Committee Has No Cybersecurity Experts," Techdirt (Sept. 2, 2016), available at https://www.techdirt.com/articles/20160902/06412735425/dhss-new-election-cybersecurity-committee-has-no-cybersecurity-experts.shtml.

109 Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity, U.S. Department of Homeland Security (Aug. 15, 2016), available at https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity.

110 Statement by U.S. Department of Homeland Security Secretary Jeh Johnson Concerning the Cybersecurity of the Nation's Election Systems, (Sept. 16, 2016) https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems.

111 Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity, U.S. Department of Homeland Security (Aug. 15, 2016), available at https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity.

112 Open Letter from the Nation's Secretaries of State to Congress, National Association of Secretaries of State, Let's Work Together to Share Facts About Cybersecurity and Our Elections (Sept. 26, 2016), available at http://www.nass.org/node/236.

113 Testimony of Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-mark-ups/hearings/task-force-election-security-securing-americas-elections-understanding (explaining that state election officials did not have sufficient time to make significant changes to their elections systems by the time DHS began to receive reports of election system targeting and engage with states in late summer 2016).

114 Open Letter from the Nation's Secretaries of State to Congress, National Association of Secretaries of State, Let's Work Together to Share Facts About Cybersecurity and Our Elections (Sept. 26, 2016), available at http://www.nass.org/node/236.

115 "NASS Statement on Cyber Security and Election Readiness," National Association of Secretaries of State (Aug. 5, 2016), available at http://nass.org/node/239.

116 Id.

117 "NASS Statement on Cyber Security and Election Readiness," National Association of Secretaries of State (Aug. 5, 2016), available at http://nass.org/node/239.

118 Open Letter from the Nation's Secretaries of State to Congress, National Association of Secretaries of State, Let's Work Together to Share Facts About Cybersecurity and Our Elections (Sept. 26, 2016), available at http://www.nass.org/node/236.

119 Letter from U.S. House of Representatives Speaker Paul D. Ryan and Democratic Leader Nancy Pelosi, and U.S. Senate Majority Leader Mitch McConnell and Democratic Leader Harry Reid to Hon. Todd Valentine, President of the National Association of State Election Directors (Sept. 28, 2016), available at https://www.politico.com/f/?id=00000157-7606-d0b2-a35f-7e1f2aac0001. See also, "States Urged to Bolster Election Security," The Hill (Sept. 30, 2016), available at http://thehill.com/policy/cybersecurity/298677-congressional-leaders-letter-to-states-bolster-election-cybersecurity.

120 Letter from U.S. House of Representatives Speaker Paul D. Ryan and Democratic Leader Nancy Pelosi, and U.S. Senate Majority Leader Mitch McConnell and Democratic Leader Harry Reid to Hon. Todd Valentine, President of the National Association of State Election Directors (Sept. 28, 2016), available at https://www.politico.com/f/?id=00000157-7606-d0b2-a35f-7e1f2aac0001.

121 Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security (Oct. 7, 2016), available at https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

122 Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security (Oct. 7, 2016), available at https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

123 Update by U.S. Department of Homeland Security Secretary Jeh Johnson on DHS Election Cybersecurity Services (Oct. 10, 2016), available at https://www.dhs.gov/news/2016/10/10/update-secretary-johnson-dhs-election-cybersecurity-services.

124 Id.

125 Letter from Hon. John Kelly, Secretary of Homeland Security, U.S. Department of Homeland Security to Sen. Claire McCaskill, Ranking Member of the Homeland Security and Government Affairs Committee, U.S. Senate (Jun. 13, 2017), available at https://www.hsgac.senate.gov/media/minority-media/senate-hsgac-staff-issue-memo-highlighting-dhs-aid-to-states-to-secure-election-systems.

126 Julie Hirschfield Davis, "Trump Says Putin 'Means It' About Not Meddling," The New York Times (Nov. 11, 2017), available at https://www.nytimes.com/2017/11/11/world/asia/trump-putin-election.html?_r=0.

127 Joint Statement from the Department of Homeland Security, the Office of the Director of National Intelligence, and the

Federal Bureau of Investigations on Russian Malicious Cyber Activity (Dec. 29, 2016), available at https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity.

128 Joint Analysis Report of the U.S. Department of Homeland Security National Cybersecurity Communications and Integration Center and Federal Bureau of Investigations, Grizzly Steppe – Russian Malicious Cyber Activity, JAR-16-20296A (Dec. 29, 2016), available at https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

129 Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent U.S. Elections, ICA 2017-01D (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf (describing the Kremlin's activities as "a significant escalation in the directness, level of activity, and scope of effort compared to previous operations").

130 Assessing Russian Activities and Intentions in Recent U.S. Elections, supra, n. 3.

131 Id.

132 Statement by U.S. Department of Homeland Security Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, (Jan. 6, 2017), available at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical. "Election Infrastructure" includes: "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments." Id.

133 Id.

134 Id.

135 Id.

136 See National Association of Secretaries of State Resolution Opposing the Designation of Elections as Critical Infrastructure (Feb. 18, 2017), http://nass.org/index.php/node/103.

137 "DHS Accelerates Work to Protect 2018 Elections Under 'Critical Infrastructure' Tag," Politico (Jun. 11, 2017), available at https://www.politicopro.com/cybersecurity/story/2017/07/dhs-accelerates-work-to-protect-2018-elections-under-critical-infrastructure-tag-159371.

138 "DHS Accelerates Work to Protect 2018 Elections Under 'Critical Infrastructure' Tag," Politico (Jun. 11, 2017), available at https://www.politicopro.com/cybersecurity/story/2017/07/dhs-accelerates-work-to-protect-2018-elections-under-critical-infrastructure-tag-159371.

139 "State election officials express frustration after meeting feds," CNN Politics (Jul. 8, 2017) available at http://www.cnn.com/2017/07/08/politics/nass-conference/index.html.

140 Id.

141 Testimony of Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Select Committee on Intelligence, U.S. Senate (June 21, 2017), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF.

142 Testimony of Chris Krebs, Senior Official Performing the Duties of the Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the U.S. Senate Committee on Armed Services (Oct. 19, 2017), available at https://www.armed-services.senate.gov/imo/media/doc/Krebs_10-19-17.pdf.

143 Id.

144 Id. See also, Letter from the National Association of Secretaries of State to Hon. John Kelly, Secretary of Homeland Security, U.S. Department of Homeland Security (Jul. 20, 2017), available at http://www.nass.org/sites/default/files/nass-letter-urgent-items-sec-kelly-072017.doc.pdf.

145 Letter from the National Association of Secretaries of State to Hon. John Kelly, Secretary of Homeland Security, U.S. Department of Homeland Security (Jul. 20, 2017), available at http://www.nass.org/sites/default/files/nass-letter-urgent-items-sec-kelly-072017.doc.pdf.

146 Id.

147 Letter from Hon. Connie Lawson, Indiana Secretary of State, National Association of Secretaries of State President to Hon. Bennie Thompson and Hon. Robert Brady (Aug. 3, 2017) (on file with Committee staff).

148 Testimony of Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-markups/hearings/task-force-election-security-securing-americas-elections-understanding.

149 Id. See also, Testimony of Chris Krebs, Assistant Secretary for Infrastructure Protection, and Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Homeland Security Committee, U.S. House of Representatives (Oct. 3, 2017).

150 Sari Horwitz, et. al., "DHS Tells States About Russian Hacking During 2016 Election," The Washington Post (Sept. 22, 2017), available at https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.27f1ff7979e6.

151 Chad Day, Associated Press, "DHS: Hackers Targeted Other Systems to Find Weak Spots," The Washington Post (Sept. 28, 2017), available at https://www.washingtonpost.com/business/technology/dhs-hackers-targeted-other-systems-to-find-weak-spots/2017/09/28/ffe1bcd0-a48a-11e7-b573-8ec86cdfe1ed_story.html?utm_term=.bab35e663963.

152 See also, Testimony of Chris Krebs, Assistant Secretary for Infrastructure Protection, and Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Homeland Security Committee, U.S. House of Representatives (Oct. 3, 2017).

153 Id. The newly-established Election Task Force includes regular participation from a number of officials within DHS NPPD's Office of Cybersecurity and Communications (e.g. Stateholder Engagement and Cyber Infrastructure Resilience and National Cybersecurity and Communications Integration Center), DHS NPPD's Office of Cyber and Infrastructure Analysis, DHS NPPD's Infrastrucutre Protection, DHS's Office of Intelligence and Analysis, DHS's Office of General Counsel, DHS's Office of Legislative Affairs, DHS's Office of External Affairs, NPPD Office of the Under Secreatry, the Election Assistance Commission, the Federal Bureau of Investigation, the Cyber Threat Intelligence Integration Center, and Office of the Director of National Intelligence.

154 Testimony of Chris Krebs, Assistant Secretary for Infrastructure Protection, and Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Homeland Security Committee, U.S. House of Representatives (Oct. 3, 2017).

155 Press Release, U.S. Department of Homeland Security, "DHS and Partners Convene First Election Infrastructure Coordinating Council," (Oct. 14, 2017), available at https://www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council. See also, Press Release, U.S. Election Assistance Commission, "Elections Government Sector Coordinating Council Established, Charter Adopted" (Oct. 14, 2017), available at https://www.eac.gov/news/2017/10/14/elections-government-sector-coordinating-council-established-charter-adopted/.

156 Testimony of Chris Krebs, Assistant Secretary for Infrastructure Protection, and Jeanette Manfra, Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Homeland Security Committee, U.S. House of Representatives (Oct. 3, 2017).

157 U.S. Const. art. I, § 4, cl. 1.

158 U.S. Election Assistance Commission, The Election Admin. and Voting Survey: 2016 Comprehensive Report, 159 (2017) https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report.pdf.

159 Lawrence Norden & Ian Vanderwalker, Brennan Center for Justice at NYU School of Law, Securing Elections from Foreign Interference, 9 (2017) https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf.

160 J. Mijin Cha and Liz Kennedy, Millions to the Polls: Poll Worker Recruitment & Training (February 18, 2014), http://www.demos.org/publication/millions-polls-poll-worker-recruitment-training.

161 Norden & Vanderwalker; Cory Bennett et al., Cash-Strapped States Brace for Russian Hacking Fight, POLITICO (Sept. 3, 2017), http://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266.

162 Brad Tuttle, How Much Election Day Costs the Country – and Voters, Time, (Nov 8, 2016).

163 Letter from Steven Simon, Secretary of State, State of Minnesota, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 25, 2017); Letter from John A. Gale, Secretary of State, State of Nebraska, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 8, 2017) (on file with author); Letter from Steve Sandvoss, Executive Director, Illinois State Board of Elections, to Tanya Sehgal, Elections Counsel, Committee on House Administration – Minority Staff (Sept. 9, 2017) (on file with author); Letter from Pedro A. Cortés, Secretary of the Commonwealth, Commonwealth of Pennsylvania, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 23, 2017) (on file with author); Letter from Connie Lawson, President, National Association of Secretaries of State, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 3, 2017) (on file with author).

164 Letter from Nellie M. Gorbea, Secretary of State, State of Rhode Island and Providence Plantations, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 25, 2017) (on file with author).

165 Letter from Gorbea, supra n. 164.

166 Letter from Cortés, supra n. 164.

167 Edgardo Cortés, Commissioner, Virginia Department of Elections, appearing at the Congressional Task Force on Election Security

168 Letter from Connie Lawson, President, National Association of Secretaries of State, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 3, 2017) (on file with author).

169 Letter from Gorbea; Letter from Simon; Letter from Gale; Letter from Marci Andino, Executive Director, South Carolina Election Commission, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Oct. 5, 2017) (on file with author); Letter from Cortés.

170 Letter from Gorbea, supra n. 164; Letter from Lawson, supra n. 168.

171 Letter from Gorbea, , supra n. 164.; Letter from Andino; Letter from Simon.

172 Letter from Matthew D. Chase, Executive Director, National Association of Counties to Leader McConnell, Leader Schumer, Senator McCain, and Senator Reed (Sept. 13, 2017) http://www.naco.org/blog/naco-supports-amendment-increase-federal-support-election-cybersecurity.

173 Letter from Secretary Steve Simon, Secretary Kim Wyman, Secretary Alex Padilla, Secretary Denise Merrill, Secretary Alison Lundergan Grimes, Secretary Tom Schedler, Secretary Barbara Cegavske, Secretary Pedro Cortés, Secretary Nellie Gorbea, and Secretary Jim Condos to Senator McCain and Senator Reed (Sept. 8, 2017) https://issuu.com/neic/docs/secretaries_of_state_letter_in_supp.

174 United States Election Project, http://www.electproject.org/home/voter-turnout/voter-turnout-data (last visited, November 1, 2017).

175 Penn Warton Pub. Policy Initiative, The Warton School, University of Pennsylvania, The Business of Voting, 11-13, 20 (2017) https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

176 Norden & Vandewalker, 9, supra n. 159.

177 Pam Fessler, Some Machines Are Flipping Votes, But That Doesn't Mean They're Rigged, NPR (Oct. 26, 2016) http://www.npr.org/2016/10/26/499450796/some-machines-are-flipping-votes-but-that-doesnt-mean-theyre-rigged.

178 Lawrence Norden & Christopher Famighetti, Brennan Center for Justice at NYU School of Law, America's Voting Machines at Risk, 5 (2015) https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

179 Center for American Progress, Election Infrastructure: Vulnerabilities and Solutions, 1 (2017) https://www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-infrastructure-vulnerabilities-solutions/.

180 Penn Warton Pub. Policy Initiative, 13, supra n. 175.

181 Norden & Vandewalker, 9, supra n. 159.

182 Matt Blaze et al., DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, 16 (2017) https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

183 Norden & Vandewalker, 9, supra n. 159.

184 Ed Felten, E-Voting Links for Election Day, Freedom to Tinker (Nov. 2, 2017) https://freedom-to-tinker.com/2010/11/02/e-voting-links-election-day/.

185 Norden & Vandewalker, 10, supra n. 159.

186 Norden & Vandewalker, 10, supra n. 159.

187 Norden & Vandewalker, 11, supra n. 159.

188 Eric Geller, Virginia Bars Voting Machines Considered Top Hacking Target, POLITICO (Sept. 8, 2017) http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492.

189 Id.

190 National Election Defense Coalition, Expert Sign-On Letter to Congress: Secure American Elections (2017) https://www.electiondefense.org/election-integrity-expert-letter/.

191 Norden & Vandewalker, 11, supra n. 159; Geller, supra n. 188.

192 J. Alex Halderman, Professor, University of Michigan, in email message to Task Force staff, Oct. 17, 2017.

193 Judd Choate, Director of Elections, State of Colorado, in person discussion with Task Force staff, Sept. 22, 2017.

194 Jake Braun, Chief Executive Officer, Cambridge Global Advisers, in person discussion with Task Force staff, Sept. 14, 2017; Larry Norden, Deputy Director of the Democracy Program, Brennan Center for Justice at NYU School of Law, in phone discussion with Task Force staff, Sept. 14, 2017; J. Alex Halderman, Professor, University of Michigan, in person discussion with Task Force staff, Aug. 9, 2017; Barbara Simons, Board of Directors, Verified Voting, in phone discussion with Task Force staff, Sept. 27, 2017.

195 Blaze, 4, supra n. 182.

196 Verified Voting, State Audit Laws Searchable Database, https://www.verifiedvoting.org/state-audit-laws/about/ (last visited Oct. 16, 2017).

197 Risk-Limiting Audits Working Group, Risk-Limiting Post-Election Audits: Why and How, 5, (Jennie Bretschneider et al. eds., 1.1 version, 2012) https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

198 National Election Defense Coalition, supra n. 190.

199 Russian Interference in the 2016 U.S. Election: Hearing Before Senate Select Commission on Intelligence, 115th Congress (2017) (testimony from J. Alex Halderman, Professor, University of Michigan).

200 J. Alex Halderman, Professor, University of Michigan, in person discussion with Task Force staff, August 9, 2017.

201 Bailey McCann, Rhode Island to Implement Post-Election Audits, CivSource (Sept. 20, 2017) https://civsourceonline.com/2017/09/20/rhode-island-to-implement-post-election-audits/.

202 Help America Vote Act of 2001, 52 U.S.C. §§ 20901-1145 (2015).

203 Norden & Vandewalker, 19, supra n. 159.

204 Callum Borchers, What We Know About the 21 States Targetted by Russian Hackers, The Washington Post (Sept. 23, 2017) https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.c296117b25d4.

205 Norden & Vandewalker, 15, supra n. 159.

206 Norden & Vandewalker, 15, supra n. 159.

207 Matthew Cole et al., Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election, The Intercept (June 5, 2017) https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

208 Norden & Vandewalker, 16, supra n. 159.

209 Id.

210 Penn Warton Public Policy Initiative, 15.

211 Blaze, 5, supra n. 182.

212 Id.

213 Steve Simon, Secretary of State, State of Minnesota, in person discussion with Task Force staff, Sept. 28, 2017; Marian Schneider, Special Adviser on Elections to the Governor of Pennsylvania, in phone discussion with Task Force staff, Oct. 13, 2017.

214 Letter from Gorbea, supra n. 164.

215 Evan Halper, U.S. Elections are an Easier Target for Russian Hackers than Once Thought, LA Times (Jul. 28, 2017) http://www.latimes.com/politics/la-na-pol-elections-hacking-2017-story.html.

216 Michael Wines, Wary of Hackers, States Move to Upgrade Voting Systems, The New York Times (Oct. 14, 2017) https://

www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html?_r=0.

217 Cory Bennett et al., Cash-Strapped States Brace for Russian Hacking Fight, POLITICO (Sept. 3, 2017) http://www.politico.com/story/2017/09/03/election-hackers-russia-cyber-attack-voting-242266.

218 Governor Cuomo Directs Cyber Security of Voting Infrastructure Amidst Reports of Foreign Interference in 2016 Election, (Jun. 20, 2017) https://www.governor.ny.gov/news/governor-cuomo-directs-cyber-security-advisory-board-review-cyber-security-voting.

219 Bennett, supra n. 7.

220 Nellie Gorbea, Rhode Island Secretary of State, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct 24, 2017.

221 Norden & Vandewalker, 14, supra n. 159.

222 Yejin Cooke, Director of Government Affairs, National Association of State Chief Information Officers, in person discussion with Task Force Staff, Sept. 12, 2017.

223 Bennett, supra n. 7.

224 Id.

225 Governor Rick Scott's 2017-2018 Budget, (last visited, Oct. 18, 2017). http://fightingforfloridasfuturebudget.com/web%20forms/Budget/BudgetService.aspx?rid1=327714&rid2=298915&ai=45000000&title=STATE.

226 Jackie Borchardt, Ohio Gov. John Kasich Vetoes Medicaid Freeze, Signs State Budget Bill, Cleveland.com (Jul. 10, 2017) http://www.cleveland.com/metro/index.ssf/2017/06/ohio_gov_john_kasich_signs_sta.html.

227 Veto Message in Brief, Sept. 20, 2017, p. 13. https://walker.wi.gov/sites/default/files/09.20.17%20Veto%20Message%20in%20Brief.pdf.

228 Voting System Standards, Testing and Certification, National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx (Jun. 8, 2017).

229 Norden & Vandewalker, 8, supra n. 159.

230 U.S. Election Assistance Commission, Managing Election Technology, https://www.eac.gov/voting-equipment/managing-election-technology/ (last visited on Oct. 16, 2017).

231 Steve Simon, Secretary of State, State of Minnesota, in person discussion with Task Force staff, Sept. 28, 2017; Marian Schneider, Special Adviser on Elections to the Governor of Pennsylvania, in phone discussion with Task Force staff, Oct. 13, 2017.

232 Nellie Gorbea, Rhode Island Secretary of State, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct. 24, 2017.

233 Edgardo Cortés, Commissioner, Virginia Department of Elections, appearing at the Congressional Task Force on Election Security.

234 Manfra, supra n. 104.

235 Matthew Cole et al., Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election, The Intercept (Jun. 5, 2017) https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

236 Id.

237 Id.

238 Id.; Ben Martin, Chief Operating Officer, VR Systems, and Mindy Perkins, Chief Executive Officer, VR Systems, in person discussion with Task Force staff, Sept. 25, 2017.

239 Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Attribution". Office of the Director of National Intelligence. Jan. 6 2017. Report. Pg. 2

240 Id.

241 Martin & Perkins, supra n. 238.

242 Id.

243 Penn Warton Public Policy Initiative, 15, supra n. 175.

244 Penn Warton Public Policy Initiative, 8, supra n. 175.

245 Penn Warton Public Policy Initiative, 8, supra n. 175.

246 Michael Riley et al., The Computer Voting Revolution is Already Crappy, Buggy, and Obsolete, Bloomberg Businessweek (Sept. 29, 2017) https://www.bloomberg.com/features/2016-voting-technology/.

247 Penn Warton Public Policy Initiative, 32, supra n. 175.

248 Julie Hirschfield Davis, "Trump Says Putin 'Means It' About Not Meddling," The New York Times (Nov. 11, 2017), available at https://www.nytimes.com/2017/11/11/world/asia/trump-putin-election.html?_r=0.

249 Testimony of Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-markups/hearings/task-force-election-security-securing-americas-elections-understanding.

250 See, U.S. Information Agency report prepared for the U.S. House of Representatives Committee on Appropriations, Soviet Active Measures in the "Post Cold War" Era 1988-1991 (June 1992), available at http://intellit.muskingum.edu/russia_folder/pcw_era/exec_sum.htm (quoting Eduard Shevardnadze, Minister of Foreign Affairs of the Soviet Union (1985-91)). See also, Testimony of Clint Watts, Senior Fellow, Center for Cyber and Homeland Security, George Washington University, before the U.S. Senate Select Committee on Intelligence (Mar. 30, 2017), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

251 Testimony of Roy Godson, Emeritus Professor of Government at Georgetown University, before the U.S. Senate Select Committee on Intelligence (Mar. 30, 2017), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-rgodson-033017.pdf (noting that even "[I]n the final years of the Soviet Union there was enough information on their

active measures systems to conclude that approximately 15,000 personnel and several billions of hard currency annually were being spent on these activities – aimed mostly at the U.S. and its allies.").

252 See, e.g., "Russia's Radical New Strategy for Information Warfare," The Washington Post (Jan. 18, 2017), available at https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.c26667e8ad3e (quoting Andrey Krutskikh, a "senior level advisor" to Russian President Vladimir Putin, for remarks at the Russian information security forum Infoforum 2016 on Feb. 4-5, 2016, asserting that Russia "has new strategies for the information arena that would be equivalent to testing a nuclear bomb and would allow us to talk to Americans as equals."). See also, "Inside Russia's Social Media War on America," Time (May 18, 2017), available at http://time.com/4783932/inside-russia-social-media-war-america/ (noting that "[O]ne particularly talented Russian programmer who had worked with social media researchers in the U.S. for 10 years had returned to Moscow and brought with him a trove of algorithms that could be used in influence operations. He was promptly hired by those working for Russian intelligence services, senior intelligence officials tell TIME.").

253 See, e.g., "Russia Election Hacking: Countries Where the Kremlin Has Allegedly Sought to Sway Votes," Newsweek (May 9, 2017), available at http://www.newsweek.com/russia-election-hacking-france-us-606314.

254 Open Hearing on Russian Interference in European Elections Senate Select Committee on Intelligence, 115th Cong. (Jun. 28, 2017), (statement of Ambassador (ret.) Nicholas Burns), available at https://www.intelligence.senate.gov/sites/default/files/documents/sfr-nburns-062817b.pdf.

255 James Ludes and Mark Jacobson, "Shatter the House of Mirrors: A Conference Report on Russian Influence Operations," Pell Center, (Sept. 26, 2017), available at http://pellcenter.org/wp-content/uploads/2017/09/Shatter-the-House-of-Mirrors-FINAL-WEB.pdf; Heather Conley and Ruslan Stefanov, "The Kremlin Playbook," CSIS, (Oct. 13, 2016), available at https://www.csis.org/analysis/welcome-kremlin-playbook; Alina Polyakova et al, "The Kremlin's Trojan Horses," The Atlantic Council, (Nov. 15, 2016), available at http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf; Christopher Paul and Miriam Matthews, "The Russian Firehose of Propaganda Model," RAND, (Dec. 13, 2016), available at https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf; and Minority Staff Report of the House Committee on Science, Space, and Technology Subcommittee on Oversight, "Old Tactics, New Tools: A Review of Russia's Soft Cyber Influence Operations," (Nov. 2017), available at https://democrats-science.house.gov/sites/democrats.science.house.gov/files/documents/Russian%20Soft%20Cyber%20Influence%20Operations%20-%20Minority%20Staff%20Report%20-%20November%202017_0.pdf.

256 See, e.g., "Don't Let Mexico's Elections Become Putin's Next Target," Council on Foreign Relations (Nov. 9, 2017), available at https://www.cfr.org/blog/dont-let-mexicos-elections-become-putins-next-target.

257 Elizabeth Weise, "After Russian election hack, U.S. security advisers form group to make 2020 race unhackable," USA Today, (Oct. 10, 2017), available at https://www.usatoday.com/story/tech/news/2017/10/10/after-russian-election-hack-u-s-security-advisers-form-group-make-2020-race-unhackable/747403001/. See also Robby Mook, "Keep the Hackers Out of Our Elections," CNN, (Aug. 24, 2017), available at http://www.cnn.com/2017/08/24/opinions/keep-hackers-out-of-our-elections-opinion-mook/index.html. See also Matt Rhoades, "Every campaign is now a cyberwar target," New York Post, (Aug. 13, 2017), available at http://nypost.com/2017/08/13/every-campaign-is-now-a-cyberwar-target/. See also Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference," Brennan Center, (Jun. 29, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference.

258 Michael O'Hanlon, "Cyber Threats and How the United States Should Prepare," Brookings, (Jun. 14, 2017), available at https://www.brookings.edu/blog/order-from-chaos/2017/06/14/cyber-threats-and-how-the-united-states-should-prepare/. See also Edward-Isaac Dovere, "Hacker study: Russia could get into U.S. voting machines," PoliticoPro, (Oct. 9, 2017), available at https://www.politico.com/story/2017/10/09/russia-voting-machines-hacking-243603. See also The Brookings Institution, "The National Security Imperative of Addressing Foreign Cyber Interference in U.S. Elections," Brookings, (Sept. 8, 2017), available at https://www.brookings.edu/wp-content/uploads/2017/09/20170908_election_security_transcript.pdf.

259 Memorandum from Eric Fischer, Senior Specialist, Congressional Research Service, on Use of Voter-Verified Paper Audit Trails by State Election Jurisdictions to Tanya Sehgal, Elections Counsel, Committee on House Administration – Minority Staff (Sept. 14, 2017) (on file with author).

260 National Election Defense Coalition, supra n. 190.

261 Blaze, 4, supra n. 182.

262 Jake Braun, Chief Executive Officer, Cambridge Global Advisers, in person discussion with Task Force staff, Sept. 14, 2017; Larry Norden, Deputy Director of the Democracy Program, Brennan Center for Justice at NYU School of Law, in phone discussion with Task Force staff, Sept. 14, 2017; J. Alex Halderman, Professor, University of Michigan, in person discussion with Task Force staff, Aug. 9, 2017; Barbara Simons, Board of Directors, Verified Voting, in phone discussion with Task Force staff, Sept. 27, 2017.

263 Norden & Vandewalker, 14, supra n. 159.

264 Juan Gilbert, University of Florida, in person discussion with Task Force Staff (Nov. 16, 2017).

265 Wines, supra n. 216.

266 Bennett, supra n. 7.

267 Letter from Gorbea, supra n. 164; Letter from Simon, supra n. 163; Letter from Gale, supra n. 163; Letter from Cortés, supra n. 163; Letter from Lawson, supra n. 168.

268 Burris, A. L., Fischer, E.A. (2016) The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election (CRS Report No. RS20898).

269 J. Alex Halderman, Professor, University of Michigan, in

person discussion with Task Force Staff (Aug. 9, 2017).

270 Risk-Limiting Audits Working Group, Risk-Limiting Post-Election Audits: Why and How, 5, (Jennie Bretschneider et al. eds., 1.1 version, 2012) https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

271 Risk-Limiting Audits Working Group, 5, supra n. 270.

272 Russian Interference in the 2016 U.S. Election: Hearing Before Senate Select Committee on Intelligence, 115th Congress (2017) (testimony from J. Alex Halderman, Professor, University of Michigan).

273 Eric Geller, Colorado to Require Advanced Post-Election Audits, POLITICO (Jul. 17, 2017), http://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

274 McCann, supra n. 201.

275 National Election Defense Coalition, supra n. 190.

276 Norden & Vandewalker, 15, supra n. 159.

277 Alia Beard Rau, Russia Tried to Hack Arizona Voter-Registration System, Federal Officials Say, AZ Central (Sept. 22, 2017), http://www.azcentral.com/story/news/politics/arizona/2017/09/22/russia-tried-hack-arizona-voter-registration-system-federal-officials-say/695057001/.

278 Norden & Vandewalker, 19, supra n. 159.

279 Yejin Cooke, Director of Government Affairs, National Association of State Chief Information Officers, in person discussion with Task Force Staff, Sept. 12, 2017.

280 Norden & Vandewalker, 19, supra n. 159.

281 Steve Simon, Minnesota Secretary of State, in person discussion with Task Force staff, Sept. 28, 2017; Marian Schneider, Special Adviser on Elections to the Governor of Pennsylvania, in phone discussion with Task Force staff, Oct. 13, 2017.

282 Cory Bennett et al., Cash-Strapped States Brace for Russian Hacking Fight, POLITICO (Sept. 3, 2017), http://www.politico.com/story/2017/09/03/election-hackers-russia-cyber-attack-voting-242266.

283 Bennett, supra n. 182.

284 Testimony of Suzanne Spaulding, former Under Secretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security, before the Congressional Task Force on Election Security Forum entitled Securing Our Elections: Understanding the Threat (Sept. 28, 2017), available at https://democrats-homeland.house.gov/hearings-and-mark-ups/hearings/task-force-election-security-securing-americas-elections-understanding.

285 Nellie Gorbea, Rhode Island Secretary of State, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct. 24, 2017; Edgardo Cortés, Commissioner, Virginia Department of Elections, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct. 24, 2017.

286 Nellie Gorbea, Rhode Island Secretary of State, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct. 24, 2017.

287 Matt Masterson, Chairman, Election Assistance Commission, in person discussion with Task Force staff, Nov. 3, 2017.

288 Nellie Gorbea, Secretary of State, State of Rhode Island, appearing at the Congressional Task Force on Election Security Forum, "Securing America's Elections: Preparing for 2018 and Beyond," Oct. 24, 2017.

289 United States Cong. House. House Permanent Select Committee on Intelligence. Open Hearing on Russian Active Measures Investigation, Mar. 20, 2017. 115th Congress. 1st session, 2017.

290 Morgan Chalfant, "Homeland Security Cyber Unit on Alert for Election Day," The Hill (Nov. 4, 2017), available at http://thehill.com/policy/cybersecurity/358710-homeland-security-cyber-unit-on-alert-for-election-day.