Debora A. Plunkett

Senior Fellow, Belfer Center, Harvard University

September 27, 2019

U.S. House of Representatives Committee on the Judiciary

Hearing: "Security America's Elections"

Written testimony of Debora A. Plunkett, Senior Fellow, Defending Digital Democracy, Belfer Center, Harvard University for the hearing of the U.S. House of Representatives Committee on the Judiciary titled "Securing America's Elections"

Friday, September 27, 2019 9:00 AM

Chairman Nadler, Ranking Member Collins and Distinguished Members of the Committee, thank you for the opportunity to testify before you today to discuss potential security vulnerabilities of our election systems and political campaigns, and solutions to mitigate those vulnerabilities.

My testimony today will focus on identifying and recommending solutions to protect democratic processes and systems from cyber and information attacks. Concrete solutions are needed to address this urgent problem. Foreign nations and non-state actors are not backing down in their efforts to hack systems, alter the outcome, and undermine confidence in our elections.

Our democracy is under attack and at risk. Threats to elections is a national security issue. We must take bold, decisive and expeditious steps to address them, and then assume that they are insufficient given the rise of nation state capabilities and intentions, and the relative known insecurities of elections systems. Threats to campaigns and candidates is also of grave concern as malicious actors have discovered and are exploiting weaknesses in the communications and technology security for candidates. Finally, there are almost certainly election system weaknesses that either have yet to be discovered or even vulnerabilities that have yet to be created, reinforcing the need for constant monitoring. All of these threats must be addressed in order to insure secure and trusted U.S. election processes.

Our elections are under attack

A core tenet of our democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it was not in reality. The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. These malicious acts revealed significant vulnerabilities in our elections process. "Russian interference operations against the United States during the 2016 presidential election were vast and complex. That's the conclusion drawn by Special Counsel Mueller, as well as by the Department of Justice, the Intelligence Community, and the Senate Select Committee on Intelligence, in the course of their respective investigations. The Russian government waged a well-documented, sustained campaign to weaken the United States, using multiple tools and tactics, damage our democracy and divide our citizens. That campaign continues today." According to the Department of Homeland Security (DHS), Russia targeted the election infrastructure of 21 U.S. states in advance of the 2016 election and were successful at penetrating a small number of them.

The 2016 election interference was not the first-time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence

Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections. This proved true during the 2018 midterm elections, where press reporting indicates that Russia used internet trolls and bots to launch and promulgate disinformation through ads on social media platforms. An October 2018 Department of Justice indictment stated that from December 2014 until at least May 2018, Russian military intelligence officer "conducted persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government."

Bad actors, whether nation states or criminals, focus on gaining unauthorized access to those systems that provide the best opportunity to achieve their individual interests, whether it be for influence, destruction, profit, espionage, coercion and just fun and fame. Regardless, in order to protect that for which our nation was created, we must focus on election security as an imperative for safeguarding our democracy. Intelligence leaders warn of ongoing and escalating interference attempts by multiple, foreign actors who view our 2020 elections as an opportunity to advance their interests at the expense of American democracy.

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.

Russia is not our only threat. In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials or attempted to interfere with state election systems. In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. As geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

Finally, while there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. The National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions

between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

Elections are administered by diverse localities

U.S. elections are decentralized and are administered by the states. The federal government provides national-level guidance, but state and local governments oversee elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters. The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. The Belfer Center's Defending Digital Democracy project conducted a nationwide security survey of states and territories, finding that the most frequent concern noted by election officials was insufficient resources to secure the process, especially in smaller counties.

It is difficult to defend the multifaceted nature of the elections processes. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique, with various intricacies in election operations. According to the National Conference of State Legislatures, the United States has over 10,000 election administration jurisdictions. These jurisdictions vary greatly in the number of voters they serve, number of personnel they employ, election infrastructure in use, cybersecurity resources at their disposal and organizational structure of election administration ownership. Additionally, these jurisdictions are relatively autonomous and have varied plans for the future of election administration under their purview. Recognizing the variety of election jurisdictions is central to developing and implementing strategies aimed at improving election infrastructure security.

Elections systems use general purpose applications

While the qualities of jurisdictions can vary significantly, there are fundamental similarities for infrastructures. Many election systems are built using general purpose technology and commercial-off-the-shelf software. While this means they are often subject to attacks popular in other sectors, it also means experts have identified best practices to mitigate many of the risks. Therefore, for many components of election infrastructure best practices for mitigating risks are largely similar to general IT security best practices.

Components of Election Systems

Election systems and components generally can be categorized into three levels of operation relating to cybersecurity risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. Finally, the third level involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.

Voter Registration Databases and Pollbooks

Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. These are typically network connected databases. The inputs to voter registration databases (VRDBs) are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state. The outputs include facilitating retrieving voter information —such as a voter verifying, they are registered, seeking a sample ballot, or finding their polling place—and transfer of voter information to pollbooks. The most common method of voter registration is through a states' DMV.

Pollbooks provide voter registration information to workers at each polling location. They are necessary to ensure voters are registered and are appearing at the correct polling place, and pollbooks being used efficiently is necessary to limit voters' wait times. Pollbooks can take the form of preprinted paper registration lists or as an electronically accessed database, known as an e-pollbook. About 48 percent of voters who cast ballots in person in 2016 were signed in at the polls by election workers using e-poll books, compared to only 27 percent in 2012.

Attacks on VRDBs and e-pollbooks could result in individuals being incorrectly allowed or denied the right to vote. These attacks could also result in confusion at the polls, undermining confidence in the integrity of elections.

Vote Capture Devices

Vote capture devices are the means by which individuals' votes are cast and recorded - the voting machines. As with other election technology, machines and process for vote capture vary by jurisdiction. Furthermore, any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate administrative decisions and voters with varied needs or preferences. For example, on election day, a polling place may give voters the choice of voting using an electronic voting machine or a paper ballot. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

The 2000 recount in Florida exposed significant limitations with punch card voting machines, which accounted for 30% of vote capture machines at the time. In 2002, Congress passed the Help America Vote Act (HAVA) which included $3 billion of funding for states to revamp their voting technology. With this funding, voting machines were replaced wholesale with more and more jurisdictions adopting mostly or purely electronic machines.

The new purely electronic machines spurred controversies of their own around whether they could be trusted to record and report votes accurately. Additionally, by the mid-2010s most of these machines had become obsolete and in 2014 the Presidential Commission on elections warned there was an "impending crisis" in voting technology. As of 2016, most of the HAVA funds that were distributed to states for the purpose of refreshing their voting technology had been exhausted. 65% states and territories in the US have less than 10% of their originally allocated HAVA funds left, another 14 states and territories (25%) had less than half of their funding left.

The Consolidated Appropriations Act of 2018 included $380 million in additional funding for election security in conjunction with the HAVA act. According to the EAC, 100% of new HAVA funds were disbursed by Sept 20, 2018. The EAC believes as of April 30, 2019, states have spent at least $108.14 million, or 29 percent of the $380 million in grant funds. A straight-line spending projection based on expenditures through the end of March 2018 suggests that states and territories will spend approximately $324 million, or 85 percent, of the funds prior to the 2020 Presidential Election. States plan to use about 28% of these funds on voting equipment.

On June 26, 2019 the House passed its FY2020 Financial Services and General Government appropriations bill which included $600 million in additional HAVA funds to be distributed to states for election security. On September 19, 2019 the Senate Appropriations Committee voted to advance its FY2020 bill which only includes $250 million for HAVA funds to be distributed to states for election security.

According to the Brennan Center for Justice, a minimum investment of $2.153 billion over the next five years is necessary to "bring all states to a reasonable baseline on election security." Contained within that estimate, is $734 million for replacing machines older than 10 years and to replace direct-recording electronic (DRE) voting machines which do not provide a paper record.

Best Practices for Securing Election Systems

The Belfer Center's State and Local Election Cybersecurity Playbook identifies ten best practices that apply to all election jurisdictions, specifically:

1. **Create a proactive security culture**. Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create a public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared. Senior election officials must lead by example, issuing guidance about the necessity of applying cybersecurity standards, stressing the importance of cybersecurity for staff and following up with operations personnel regarding the implementation of improved cybersecurity protections. Developing a detailed cyber incident response plan and mandating frequent testing of critical systems will ensure both resilience and comfort with crisis management. There is a wealth of expertise available to support improving cyber defense capabilities. Election officials should leverage these resources to complement their in-house expertise. Finally, election officials must be diligent in selecting those who will be involved in election administration. Background checks should be conducted on all personnel accessing sensitive information and privileged systems, and vendors should be required to do the same.

2. **Treat elections as an interconnected system**. Adversaries can target not only individual parts of the election process but also the connections between them. Attackers look for

seams: they seek the weakest point and move from three to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet because attacks can be executed using mobile storage devices (e.g., thumb drives) or other external storage devices. Any computer or other digital device that touches election processes must be safeguarded. Device security management should be centralized and streamlined by incorporating election offices into existing technology security plans.

3. **Require a paper vote record**. To protect against cyber attacks or technology failures that could jeopardize an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software and data; every aspect from the ballot displayed to the voter to the recording and reporting of the votes, is under the control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or event to detect that an attack has occurred) after the fact. As a result, an auditable paper record must be created for every vote cast that is verified by the voter and the paper record must have a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.* Auditing should be embedded at points in the process where data integrity and accuracy are critical; for example, with voter registration records. Post-election audits should be standard practice, using paper records to confirm electronic results

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system. Strong passwords must be required not only for official accounts but also for key officials' private email and social media accounts.
6. **Control and actively manager access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to

succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them. As a result, there should be a limit on the number of people with access to the system with a focus on providing access to those who need it to complete their jobs. Additionally, using the principle of 'least privilege' will restrict what each user is authorized to do, giving the minimal level of access required to perform their jobs. Finally, anyone who no longer needs access, regardless of their privilege level, should be quickly removed from access. This should be a standard offboarding procedure.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials should consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems first. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs. Devices with sensitive data should be configured to only be used for their specific purpose in the elections process, and the use of removable media devices (e.g. USB/thumb drives) should be restricted and carefully monitored.

8. **Monitor, log and back up data**. Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross country patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs. Backups should be regularly performed, should be read-only once to prevent data corruption, and should be regularly tested by performing a complete restoration from backups. Backups should also be stored in a different physical location than the master database and should be physically secured.

9. **Require vendors to make security a priority**. Vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. A Belfer Center study found that 97% of states and territories used a vendor in some capacity. Some vendors service multiple states— meaning an attack on one vendor could affect many elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. Specific and explicit security specifications and standards should be written into contract proposals, acquisition documents and maintenance contracts to ensure that vendors follow sufficient security standards and guarantee state and local governments' ability to test systems and software. Vendor security commitments should be independently verified and periodically tested. Finally, vendors must be required to provide notification of any system breach immediately after they become aware of it.

10. **Build public trust and prepare for information operations.** Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. Communicate with the public to reinforce the message that integrity is a top priority. Start informing the public about cybersecurity threats before elections are held. Include the steps taken to counter the threats and readiness to respond in the event of an attack. Establish processes and communications materials to respond confidently and competently in the event of an attack. Build relationships with reports, influencers and key stakeholders to establish trust and have good communications channels before an incident occurs. Finally, routinely monitor social media, email accounts, and official websites and establish points of contact with social media firms.

Conclusion

To protect our election systems, it is imperative that we prepare, protect and persist. In preparation, we create a culture of security by establishing clear ground rules from the top down, discuss security policies with those who have access to systems, and minimize any weaknesses in people, processes, or technology. Protect involves building resilience by instituting the strongest defenses that can be afforded, and then ensuring a layered approach to security to minimize the potential for easy access with little effort. Finally, persistence is all about vigilance. Developing plans ahead of time, practicing them before game day, and reviewing the plans after implementation are critical steps. Adversaries are diligent, too!

Election systems must be treated as critical infrastructure. This means that there must be appropriate levels of investment. Also, there must be mechanisms for collaboration among states/local jurisdictions with established information sharing channels. Additionally, there is a need for process(es) to share and act on critical threats; checks and balances on appropriate installation of equipment; requirements for vendors to deliver systems free of known vulnerabilities, and to meet specific security standards (back-ups, software assurance, etc.).

Finally, the Federal Government must provide requisite support for elections by allocating resources to upgrade election systems to the highest security standards; insuring information exchanges between federal, state and local entities is seamless, timely and relevant; instituting security standards that vendors must follow for election systems or components used for such systems; and enforcing a culture of security by acknowledging the threat and keeping the American public fully informed on malicious actors, intentions and the government's efforts to eradicate them.