20 for 20

20 Ways to Protect the 2020 Presidential Election

David Levine, Elections Integrity Fellow, Alliance for Securing Democracy
Matthew Weil, Elections Project Director, Bipartisan Policy Center
May 20, 2020

Introduction

At the end of 2019, the federal government appropriated for states $425 million in Help America Vote Act (HAVA) election security grants to improve the administration and security of federal elections. These grants followed $380 million provided to states at the beginning of 2018. Since these funds were allocated, there has emerged a consensus that states should spend at least a portion of the money on securing the 2018 midterm and 2020 presidential elections in an effort to prevent a repeat of Russia's interference in the 2016 presidential election.

Then, the coronavirus pandemic came ashore in the midst of our presidential primary. It led some states to begin using previously appropriated election security funds to cover unanticipated costs stemming from the virus, such as preparing for a surge of mail-in ballots, buying protective equipment for poll workers, and disinfecting voting machines. Wisconsin's last-minute decision to hold an-in person presidential primary election on April 7th—which resulted in mass confusion, thousands of voters waiting in hours-long lines, problems adapting to the surge in absentee ballot requests, significant shortages of both poll workers and polling places, and many voters and poll workers testing positive for coronavirus—may lead more states to use election security grants for virus-related election preparations.

Modifying election plans to account for coronavirus is understandable and essential. However, drawing on pre-existing election funding to address these modifications presents a particular dilemma: ahead of the presidential election, our nation's election infrastructure is not yet fully secure, while America's adversaries continue to possess the capabilities to exploit technical deficiencies and to try to influence public sentiment and shape voter perceptions. In March, the federal government allocated $400 million to help states bolster their efforts to ensure the integrity of the upcoming 2020 elections in response to the coronavirus—an important first step.

However, as a bipartisan group of secretaries of state recently acknowledged, states will need much more dedicated election security funding to prepare for the remaining 2020 elections, including defending the presidential election against attempts to undermine it.

This paper, *20 for 20*, provides 20 ideas that more states could implement to help further protect the 2020 presidential election with additional funding. Some ideas are based on successful practices states developed using previous federal funds, while others are based on feedback from voters. Additional ideas came from local election officials, as well as others with relevant experience, such as the members of the Election Infrastructure Security Subsector Government Coordinating Council (EIS GCC), which developed a document this March on how state election officials can use the 2019 funds more broadly. These ideas illustrate what election officials have been doing—and can hopefully continue doing—to protect the 2020 presidential election from foreign adversaries, as well as other ideas for final preparations before the voting commences.

1. Develop and conduct more frequent threat assessments

As cyber threats evolve, state election officials need to know where new vulnerabilities might emerge in their state's election infrastructure. This awareness will not only help state officials assess the present security of their infrastructure, including how effectively officials use and maintain the infrastructure, but will also allow states to implement mitigation strategies to address the identified weaknesses, so that malicious actors are less able to exploit them and undermine our elections. A number of these strategies are described in detail below.

2. Hire additional cybersecurity staff

After U.S. intelligence agencies determined that the Russian government was behind cyber attacks and covert social media operations intended to influence the 2016 presidential election, many states hired staff to bolster their election security. More could do so with additional funding. For example, in September 2019, Michigan's secretary of state hired the state's first-ever full-time elections security specialist to coordinate the state's overall security plan, and work with state and federal partners to assess, train, and communicate with local election officials on election security best practices. Earlier this year, the Ohio secretary of state's office hired a chief information security officer to oversee its election security efforts, as well as those at each of Ohio's 88 counties.

Such hires can assist state and local election officials with security incident management and response, security threat and vulnerability management, risk management, security administration, security education and training, security publications, and special security projects and/or investigations. Additional federal funding would not only help facilitate the hiring of more cybersecurity staff, but could help to ensure their retention to address future vulnerabilities.

3. Mitigate the potential risks associated with administering more voting by mail due to the coronavirus

Vote-by-mail presents more opportunities for votes to be lost, tampered with or intercepted than does in-person voting, even though perceptions of the vulnerabilities far outpace reality. Mail ballot processes often rely on the U.S. postal system to (1) deliver a mail ballot request from the voter to the local jurisdiction; (2) deliver the unmarked ballot from the jurisdiction back to the voter; and (3) deliver the marked ballot back to the election jurisdiction for counting. Even if all of these steps are completed, slower-than-expected mail delivery can lead to voter disenfranchisement, which foreign adversaries could try and use as fodder to undermine confidence in our democratic institutions and processes.

With additional funding, more states could follow the example of states like Washington, where each ballot envelope has a unique barcode and tracking system that election officials and voters can use to monitor a ballot's progress via an online portal. Providing this service not only helps bolster election security but also gives voters more confidence that their mail-in ballots will count.

4. Ensure that all election officials in the state use multi-factor authentication

Added layers of security are imperative when accessing sensitive data or systems such as election offices' social media accounts and voter registration databases, which Russian government-affiliated cyber actors targeted in the run up to the 2016 U.S. elections. Multi-factor authentication is a digital authentication method that requires two or more distinct factors for successful authentication. The three authentication factors are something you know (e.g. password or PIN), something you have (e.g., a passcode sent to or generated by a device), and something you are (e.g., a biometric, such as a fingerprint to unlock the phone).

In Washington state, all users of the state's voter registration system are required to use two of these factors to successfully authenticate their accounts. This strengthens the security of individual user accounts by using a secondary device to verify everyone's identity. It also makes it more difficult for anyone but the user to access an account even if a nefarious actor has the user's username and password.

5. Help local election officials adopt HTTPS website security measures

HTTPS is a standard security protocol that makes it much harder for an adversary to hijack a website and provide false information. Particular areas of concern include the release of unofficial election results and the diversion of voters to phony sites that mimic real ones and steal voters' information. Voters already have a difficult time determining trusted sources of information, and these attacks could create broad doubt about the legitimacy of the voting process. In a recent survey of county websites and county election administration websites in the 13 states projected as battlegrounds in this November's presidential election, a majority lacked HTTPS website security measures. Of the states surveyed, Arizona had the highest percentage of HTTPS protection with 80 percent, and Texas has the lowest at 22.8 percent.

6. Assist state and local election officials with maintaining safe cybersecurity practices while transitioning from offices to remote workstations

In response to the coronavirus, organizations all over the world are scrambling to purchase and set up remote work stations for employees, and election officials are no exception. Each election official that has remote access to a work computer should have a secure Virtual Private Network (VPN). A VPN connection is critical for maintaining full end-to-end encryption when connecting to a remote computer. It is also important that all employees are trained and educated about protecting sensitive information while working remotely. For example, if an official is working from a public location like a coffee shop, he/she should avoid using free Wi-Fi. Instead, they should use a personal hotspot, which is more secure, and be sure to disable mobile Wi-Fi and Bluetooth when not in use to prevent connecting to unknown networks or peer-to-peer devices.

7. Take steps to protect voter registration databases from ransomware attacks

Hackers have shut down municipal computer systems in Texas, Maryland, and New York, and threatened to erase databases unless the cities pay ransom. If there are similar threats targeting state voter registration systems, for example, voters could be prevented from registering to vote and poll workers could be prevented from confirming voter eligibility, both of which could undermine public confidence in the election itself.

With additional funds, states can take steps to reduce this threat, though, it may be too late to move entire databases before the November election. Steps could include moving the voter registration database to a dedicated network, as Illinois did after its voter registration system was successfully penetrated by hackers affiliated with the Russian government in 2016, offering security awareness training for election officials, and/or providing funding for improved devices and software. For example, Wisconsin requires local election officials to authenticate their identities with a physical token, called a FIDO key, when they log into state systems.

8. Conduct a proactive voter education campaign

Engaging with and explaining to voters the steps states and localities are taking to secure the presidential election has taken on new importance in the current pandemic environment. According to a NPR/PBS Newshour/Marist Poll earlier this year, 41 percent of Americans believe the United States is “not very prepared” or “not prepared at all” for the November 2020 presidential election; 59 percent of those surveyed reported that it is hard to tell the difference between what is factual and what is misleading information; and 55 percent of Americans say it will be harder to identify deceptive information than it was in 2016.

These figures pre-date the coronavirus outbreak; it is possible that lack of confidence is now higher. This is why it is so important to mobilize the most trusted voices in local communities to conduct voter education campaigns. Sixty-eight percent of the survey respondents said they are confident that their local election officials will run a fair election. Local election officials are the most trusted sources for election information and should be at the forefront of state and local efforts to communicate with voters.

9. Create a cyber navigator program

After hackers affiliated with the Russian government successfully penetrated its voter registration database during the 2016 presidential election cycle, Illinois started the first of these programs, employing cybersecurity experts with responsibility for geographic zones across the state to work with local election officials to conduct comprehensive risk assessments of each jurisdiction. This included a review of the organization’s security controls; analysis of system and network documentation for accuracy; and the provision of guidance regarding software patches, system updates, email, and security software. Such a program can help states identify and locate their vulnerabilities: as a result, a number of other states have followed Illinois’ example.

10. Use a social media monitoring service to help fight disinformation and/or misinformation efforts

Shortly before the Iowa Caucuses, the legal advocacy group Judicial Watch falsely claimed that eight Iowa counties had more voter registrations than citizens. Despite efforts by Iowa’s secretary of state to debunk these falsehoods by pointing to public county-by-county voter registration totals, the claims were repeated by some major media outlets, such as The Epoch Times. They also went viral on social media, before Facebook eventually put up warnings on several posts stating that the Judicial Watch claim contained false information.

State and local election officials have options to combat disinformation and misinformation efforts. Colorado uses two different social media monitoring services to help counter efforts like this: the "Dumb/Not Smart" program, which aggregates social media data, and a "Smart" program, into which state officials enter correct information about the election and the software identifies incorrect information being disseminated on social media.

11. Assist local election officials with assessing and improving their physical election security

The U.S. Department of Homeland Security employs physical security specialists who, upon request, will conduct physical security checks of state and local election offices to ensure they are sufficiently secure from active shooters, unauthorized visitors, and other potential threats. With additional funds, states can help facilitate these security checks as well as any upgrades advised by DHS inspectors. This should reduce the physical risk to a state's elections systems and facilities.

12. Help local election officials work with Facebook and Twitter to be identified as trusted sources

Since large swaths of the electorate have difficulty determining whether information they read is misleading, they must be encouraged to seek out trusted sources, such as their state and local election officials. One way this can be reinforced is by working with local election officials to help ensure that Facebook and Twitter are verifying these officials as trusted sources on an expedited basis. Both Facebook and Twitter provide verified badges for accounts that are in the public interest, notable, complete, unique, and authentic.

13. Further protect the state's voter registration database from bad actors

States using voter registration databases that are more than a decade old are susceptible to cyberattacks. If successfully breached, hackers could alter or delete voter registration information, which in turn could result in eligible Americans being turned away at the polls or prevented from casting ballots that count.

At this juncture, there may not be enough time for states to buy and implement new, more secure voter registration systems before the 2020 presidential election, but there should be enough time to upgrade their systems to help avoid a repeat of 2016. For example, earlier this year, the Iowa secretary of state and chief information officer's office teamed up to implement an application that allows them to track changes to the voter registration database and flag anomalies. With additional funds, more states could invest in similar tools to protect their databases against erroneous changes, detect intrusions or unwanted modifications, and recover from any issues once detected.

14. Strengthen electronic poll book (EPBs) procedures

States that use EPBs—laptops or tablets that contain a list of eligible voters in the district or precinct—should have backup paper poll books ready to deploy to every polling place at the time voting begins. Unfortunately, not all states that use EPBs on election day have paper backups. EPBs have a number of benefits, such as expediting the vote check-in process, but they present risks. For example, electronic pollbooks that are networked to one another via wireless communication are susceptible to an attack that either shuts the network down or alters the data on the pollbooks. As a result, every jurisdiction that uses them should have paper backups ready in case they malfunction. This not only helps protects the integrity of the election, but helps ensure that voters are not turned away or forced to wait for extended periods of time if an EPB becomes inoperable.

15. Ensure that local election officials have enough provisional ballots and related materials

If an EPB fails, it may not be possible to determine a voter's eligibility, particularly if the backup paper pollbook is unavailable or found to contain errors. Provisional ballots help ensure that individuals can cast a ballot while providing election officials time to determine eligibility.

Provisional ballots offer a failsafe so that election officials can determine voter eligibility after Election Day. Election officials need to have enough of these ballots to enable voting to continue even in the event of system failures. Voters should not have to wait more than 30 minutes to cast a ballot following a system failure.

16. Conduct a post-election tabulation audit

In an ideal world, more election officials would conduct risk-limiting audits (RLAs), as Colorado and Rhode Island, among others, will do for the 2020 presidential election. Such audits are the gold standard to ensure that voting equipment is working properly and ballots are counted as cast. However, as the National Academy of Sciences alluded to in its 2018 report, Securing the Vote: Protecting American Democracy, it could take up to a decade to fully implement RLAs across the United States.

For now, conducting a random post-election tabulation audit for even a small percentage of ballots cast can help to thwart foreign attempts to meddle with the election result. It can detect problems with ballot counting and increase voter confidence in the voting and tabulation equipment and in election outcomes. This recommendation is only applicable for states and jurisdictions that use paper ballots.

17. Following the 2020 primary elections, conduct statewide tabletop exercises to prepare for the general election

These preparations can help state and local election officials receive additional practice in responding to different types of disaster scenarios that could disrupt the 2020 presidential election, including coronavirus. For example, the U.S. Cyber Infrastructure and Security Agency (CISA) conducted two election infrastructure tabletop exercises in August 2018 and June 2019 that helped state and local election officials, as well as their partners, collaborate and identify best practices and areas for improvement in election-related cyber incident planning, identification, response, and recovery.

Funding similar statewide exercises can help to assess election officials' readiness for different potential disruptions, instill good habits for responding to them, and identify additional gaps that can be addressed before the 2020 presidential election.

18. Help localities transition all government websites, including the election sites, to ".gov" domains

Many local election officials' websites do not have ".gov" web addresses, which means the federal government has not verified their authenticity and voters cannot clearly tell whether the information on them is from an actual government agency.

It costs about $400 per year to have a ".gov" domain. If cost is an impediment for local governments needing to make this transition, states should offer to help, as Iowa has vowed to do. The U.S. Department of Homeland Security recommends all government entities use the ".gov" domain, and the National Association of Secretaries of State adopted a similar resolution in February 2020.

19. Acquire the most current, secure operating system available

Many election systems or back office systems are running on a Windows 7 or older operating system, which are no longer supported by Microsoft. If these systems cannot be upgraded, it is important that states and localities purchase Microsoft's extended service. Even simpler, the best defense against viruses and malware is to update to the latest security software, web browsers, and operating systems.

20. Provide updated guidance on securing election infrastructure in light of coronavirus

For example, if localities are preparing to conduct an election with significantly more mail-in ballots than in previous years, states should offer localities guidance on vote-by-mail best practices concerning technology, counting, and ballot distribution and collection. For example, it would be best for states to offer secure drop boxes in accessible locations for voters to drop off ballots directly.

Conclusion

The U.S. intelligence community's unanimous assessment is that foreign actors will seek to interfere in the 2020 elections. All indications are that they have already started. Focusing on protecting elections and voters from the coronavirus is essential but should not happen at the expense of preventive measures against foreign interference in U.S. elections. Indeed, Congress should allocate sufficient funding to manage coronavirus-related preparations without states having to encroach on preexisting election security funds.

Providing the necessary funding to protect American elections against foreign interference, especially during this pandemic, should be a national security priority that unites both major political parties and all citizens. The ideas proposed in this paper would make American elections safer and protect public confidence in their legitimacy, but they require more resources to be achieved. Preparing for an election does not happen quickly; it started long ago. Still, with additional funding, state and local election officials can adopt at least some of these recommendations in time for the presidential election.