Testimony of Matthew Masterson
U.S. House of Representatives
Homeland Security Committee
Subcommittee on Cybersecurity, Infrastructure Protection & Innovation
"Securing Democracy: Protecting Against Threats to Election Infrastructure & Voter Confidence"
January 20, 2022

Chairwoman Clarke, Ranking Member Garbarino, and members of the Committee,

The 2020 U.S. election was unprecedented in American history. While many have detailed what went wrong (or right), reports have largely overlooked the group most impacted by these changes: state and local election officials. Election officials anticipated problems, quietly pivoted with each changing health measure and court case, and faced many of the worst repercussions of viral and inflammatory misinformation. In the end the 2020 election was secure and accurate because of their hard work and commitment to our democracy.

Trust in American elections is under attack from abroad and at home. The federal government's support framework, while improved, remains challenged to effectively ameliorate the issues election officials face. The threats are real and evolving. Immediate support and investment must be provided to these officials in advance of the upcoming midterm elections and the 2024 Presidential election.

Threats to Election Processes[1]

1. Election officials' capacity to do their jobs is degraded by physical threats and broad distrust fomented by bad-faith actors. These threats undermine officials' ability to conduct critical community outreach, and could contribute to brain-drain at a time when competence at the local level is needed most.

2. The playbook for undermining confidence in election results is well-defined and available for foreign and domestic influence agents. The 2020 election prominently featured attempted election interference from foreign and domestic actors. Influence agents are emboldened by 2020, while defenders of election integrity are under-resourced and uncoordinated, leaving them vulnerable to repeated tactics.

3. Inconsistent funding and lack of governance structures around elections IT continue to perpetuate vulnerabilities. Despite marked progress since 2016, emerging threats such as ransomware continue to expose critical election systems to crippling attacks. In defending election systems, under-resourced local governments face off daily against well-funded nation-state adversaries, a disparity that continually exposes election systems to attack.

[1] This testimony is based in large part on a Stanford Internet Observatory research paper: "How to Secure American Elections When the Losers Won't Accept They Lost" by Matt Masterson,Jennifer Depew, Katie Jonsson, Shelby Perkins, Alex Zaheer.

Recommendations

In light of the aforementioned threats, and others yet to come, below is a set of concrete and actionable recommendations to shore up election security and ensure election confidence. Each of these recommendations will require coordination by relevant stakeholders at the local, state and federal level.

Fund elections consistently at the state, local and federal level.

Every year, state and local election officials across the country struggle to obtain the funding needed to run elections. State and local governments often push aside pleas in favor of issues perceived as more immediate, passing over electoral needs that are commonly viewed as seasonal despite elections that are run several times a year in most jurisdictions. Almost every election official is commonly asked “What do you do the other 364 days a year?” when discussing the operational challenges of their work.

Securing election infrastructure is a matter of national security. This is precisely why the Department of Homeland Security designated election systems as critical infrastructure in 2017. Elections should be funded commensurate with their status as critical infrastructure, with all levels of government ensuring regular and consistent funding. A shared funding structure should be implemented in which all levels of government pay for their portion of each election. This practice is done locally in several states and is sometimes referred to as “charge backs” or the “ballot real estate” model. The idea is that each jurisdiction that appears on a ballot in any given election is charged for its portion of that election. For instance, if an election has a congressional race, state house race, mayor’s race and county commissioner race, then the federal government would pay for the cost of the house race, state government for the cost of the state house race, city government for the mayor’s race and the county for the cost of the commissioner’s race. This would ensure consistent and regular funding of elections, with each level of government paying its share of the cost.

Congress should establish an elections fund, administered by the U.S. Election Assistance Commission (EAC), that state election officials can draw down from based on the expense to run federal elections in their state. States should be required to pass the majority of the money down to their local officials to cover the additional costs of running federal elections. This funding structure will incentivize deliberative, planned investment that allows for risk-based decision-making and funding for human capital, systems acquisition and processes to ensure sustainability of those systems over time.

Ensure the physical security of election officials, offices and staff across the country.
Many state and local election officials faced threats of violence due to mis- and disinformation about the 2020 election. In many cases, officials who reported these threats received little to no support from local, state or federal law enforcement officials. Many of the threats were deemed not serious or imminent enough to necessitate action.

More must be done to protect the health and safety of election officials and election workers, including private sector employees who support elections. The recent creation of an Election Threats Task Force at the Department of Justice (DOJ) is an important and encouraging first step. The following steps to further protect election officials:

1. **Publication and use of threat data**: The DOJ Election Threats Task Force should provide data after each federal election regarding the scope and scale of threats against election officials and workers. This report should include the number of complaints, number of credible threats, number of acts of violence and number of prosecutions for those threatening election officials or workers. This data would support efforts at the state and local level to prioritize funding for physical security, shore up gaps in security and better diagnose ongoing problems. In addition, based on this data, the DOJ task force, in coordination with CISA, should release guidance on best practices for election officials, counties, states and the federal government to better protect those who run elections.

2. **Increased information-sharing regarding threats**: From our interviews with election officials, it became clear that federal, state and local law enforcement are not sufficiently coordinated regarding the scope, scale and regularity of threats against election officials. This is particularly concerning because existing structures are in place, including state fusion centers, to facilitate this information-sharing. In order to ensure comprehensive data is collected, analyzed and shared, local and state law enforcement should be required to share activity directed against election officials and workers with federal law enforcement in their state. In return, federal law enforcement should regularly report back to state and local officials regarding the activity in their jurisdiction with full transparency regarding any actions taken, including if investigations have been initiated.

3. **Penalties:** Congress and state legislatures should pass laws offering harsher penalties for threats or acts of violence against election officials. Following the 2020 election, there have been few consequences for those who threatened election officials. Any potential violence against election officials or workers should be treated as a threatened attack on the process and democracy itself, and should result in criminal liability.

4. **Privacy:** Many threats against election officials and staff directly target their homes and families. More must be done to protect their private information from would-be malicious agents. Many states have passed laws that protect the identity of certain subsets of registered voters. These categories typically include law enforcement officers, judges and domestic abuse victims. Election officials should be included in this category to ensure that their personal information is not readily available publicly.

5. **Prioritizing protection of election officials and workers:** State and local law enforcement should treat threats against election officials as credible. This may mean increasing patrols around offices and residences, as well as further investigation into additional threats. Because state and local law enforcement often lack sufficient funding,

state legislatures and county governments should provide additional funding to support the protection of election offices and workers, especially during and after election periods.

6. **Physical security and doxxing training:** CISA should offer training and guidance on physical security and doxxing prevention measures. CISA has protective security advisors (PSA) located across all 50 states to advise on physical security matters. These PSAs have done a great job working with local election officials to evaluate the physical security posture of local offices and storage facilities. PSAs should offer additional support and training to help election officials protect themselves and their staff from doxxing and physical harm away from the office.

Encourage states to implement paper-based pre-certification audits.

No single improvement to the security of elections was more important in 2020 than the widespread use of auditable paper ballots. Approximately 95% of votes cast in the 2020 election were on an auditable paper ballot, up from just over 85% in 2016. In Georgia, election officials could hand-audit ballots to show the accuracy of the election results. In Maricopa County, Arizona, the election officials conducted the state-required public hand audit by bipartisan recount boards. The results of this hand audit affirmed the results of the election in the county.

States should prioritize implementation of paper ballot audits that are completed before vote counts are certified. These audits should offer a transparent, bipartisan and repeatable process by which the results of the election as tabulated by the voting systems can be evaluated through the review of the paper ballots.

In pursuing better, more efficient pre-certification audits, states should also continue to pursue evidence-based elections. This means implementing systems, processes and procedures that maintain transparent records of the integrity of the election. An audit is only as good as the integrity of the artifacts to be audited. For elections, this means that chain of custody of the ballots and proper ballot manifests are imperative to the trustworthiness of the audit. As part of the implementation of these post-election audits, states should support local election offices in implementing consistently documented chain of custody and ballot tracking procedures across the state.

Reform the federal voting system certification process.

The process for voting system testing and certification must be reformed. Election officials have been forced into maintaining outdated and unsupported systems for longer than their expected lifespan in part because the EAC process has not evolved to support items like component certification, regular patching of systems and further deployment of commercial off-the-shelf technology. While EAC commissioners have committed to the pursuit of these items as part of the rollout of the Voluntary Voting System Guidelines (VVSG) 2.0, the passage of VVSG 2.0 as the same monolithic standard as the prior VVSG makes it unlikely that the process can be reformed enough to be responsive to the needs of election officials.

Congress should further clarify the roles of EAC and CISA in elections, making CISA the technical lead while allowing the EAC to better focus on its other election administration missions. Both EAC and CISA have limited resources and capabilities, so further clarification of roles and responsibilities would allow each agency to best use its time and money in support of the election community. CISA is the more technically capable organization and should be formally designated as the lead federal agency for the physical and cybersecurity support of election systems and officials. This should include moving the federal Voting System Testing and Certification Program to CISA. The National Institute of Standards and Technology (NIST) should remain in its HAVA-created role as technical consultant on the development of the VVSG.

The EAC should be empowered to focus on all other aspects of the election process beyond cyber and physical security issues, allowing it to build out its clearinghouse function, advancing data collection and research efforts, and continuing to disperse election grants provided by Congress. Creating well-defined responsibilities for CISA and EAC will allow both agencies to fully achieve their core missions, eliminating the ongoing federal infighting regarding roles and responsibilities and creating clear lines of communication for election officials on these issues.

In addition, regardless of who runs the program, the federal testing and certification process should be reformed to address the marketplace challenges it is creating:

1. **Already certified voting systems running unsupported operating systems should be decertified**. Because these systems are running unsupported operating systems, they are unable to be patched to remediate known vulnerabilities. Most of these systems cannot simply be updated because they lack the memory or processing power to run updated operating systems. Many election officials running these systems have expressed the need to replace them, but have not received the necessary funding to do so. Voting system vendors and election officials should be notified of pending decertification and should be given enough time to upgrade or replace their systems.

2. **VVSG 2.0 should be implemented rapidly**. This would mean that all new systems submitted to the certification program must be VVSG 2.0-compliant to receive certification by a date established by the EAC in the near future. The certification program should avoid using metrics like accreditation of the voting system test laboratories to conduct VVSG 2.0 testing or certification of the first voting system to VVSG 2.0 as metrics for sunsetting VVSG 1.0 and 1.1. In setting a date, the certification program should publish a definition of what constitutes a new voting system and make clear that this definition will be enforced. In the past, vendors have avoided certification to the newest standards, such as VVSG 1.1, by modifying already certified systems, allowing them to be tested to the older standard in perpetuity.

3. **The certification program must incentivize patching of voting systems**. Currently, the certification process disincentivizes regular patching of systems by requiring testing

(sometimes extensive) of most software updates. This causes voting system vendors to hold off on pursuing modifications to systems until they reach a critical mass of changes that justify the financial and time costs associated with certification. Instead, the certification program should revise its policies to allow vendors to attest to their own testing of critical patches on already certified systems. In allowing for vendor attestation, the certification program should require the voting system test laboratories to review and approve vendor testing documents prior to approval of the patch. This process should be expedited to allow for timely deployment of patched systems to the field, recognizing that the majority of voting systems cannot be remotely patched. This process would be separate from the existing de minimis change process, which requires no additional testing by the vendor or test lab to receive approval.

Provide election offices more scalable and proactive services through CISA and EI-ISAC.

Given the vast and decentralized nature of election administration in the United States, the challenge for CISA and the EI-ISAC is immense. How do you ensure that information, support and services reach the smallest town in Wisconsin or the most remote county in Montana? Even if you reach those places, how do you make the information and services relevant and usable for the election official in Jackson County, Ohio? CISA and the EI-ISAC have made incredible progress on this challenge since the 2016 election. All 50 states, Washington, D.C. and the four territories joined the EI-ISAC; intrusion detection sensors were deployed on election infrastructure across all 50 states; thousands of state and local offices participated in tabletop exercises; hundreds of cyber hygiene scans were conducted; and virtually every state received a penetration test.

Even with the success of these offerings, the scalability of the services remains a challenge. Due to resource constraints, CISA can only perform a finite amount of onsite vulnerability assessments of all critical infrastructure, let alone elections. In addition, many election offices do not have the necessary IT resources to benefit from some of the more in-depth services. Over the last four years, CISA has learned the intricacies of the election sector and the systems that support it. It has worked to prioritize the services that are most useful, and it has developed new and scalable services, such as remote penetration testing, to better serve the community.

In 2020, CISA recognized that it needed to be more proactive in its work with election officials. In collaboration with the Defense Digital Service, the agency developed and released a tool called Crossfeed, which is used to gather information about vulnerabilities on public-facing systems supporting critical infrastructure. Crossfeed proactively collects data through a variety of open-source tools, publicly available resources and data feeds, and can operate in a “passive” mode where it relies on unintrusive data-gathering methods.

Moving forward, CISA and the EI-ISAC should learn from the success of Crossfeed to identify and provide additional proactive, scalable services to local election offices. Both entities have built a level of trust with election officials that means they can afford to be more aggressive in the types of support provided. For example:

1. **CISA should expand the Crossfeed program**. Recently CISA announced the continuation of Crossfeed. This is an important first step. The agency should expand the use of the program to include offering all 50 states, D.C. and the territories active participation in the program with the goal of proactive monitoring of publicly available aspects of state and local offices' infrastructure. This should also include the use of Crossfeed on other election-specific technology, such as proactively searching for voting systems that may be inadvertently connected to the Internet. Further, CISA should offer the service to election vendors, campaigns and other election-related entities.

2. **CISA should offer remote hunt and incident response to election offices.** Like onsite vulnerability assessments, CISA hunt and incident response services have traditionally involved onsite deployment of responders to an office. This makes both services extremely labor-intensive and difficult to scale. CISA has piloted some remote incident response capabilities in the past, and it is time to expand this effort along with proactive network hunt capability.

3. **EI-ISAC should expand its endpoint protection program**. Throughout 2020, EI-ISAC worked with some state and local offices to pilot endpoint protection for their offices. This pilot proved to be useful for both the election officials and EI-ISAC as it worked to gain greater insight into the scope of activity targeting election infrastructure. This program should be expanded to more jurisdictions, with a focus on medium to small localities that lack the same or similar capabilities and would benefit most from these services.

4. **EI-ISAC should offer cloud-based email as a service to local election offices.** Email security is one of the largest risk areas for local election offices. Many continue to run outdated and unpatched email servers with little ability to upgrade and maintain them. EI-ISAC should partner with Microsoft, Google or other large cloud-based email providers to explore implementation of email as a service for local election offices and county governments. For counties that are unable or unwilling to implement a state-based solution, the EI-ISAC could be a viable solution from a trusted partner.

5. **EI-ISAC should provide a managed solution for multi-factor authentication (MFA).** Many election offices continue to struggle to implement MFA across their systems. While there are a lot of MFA solutions available in the marketplace, many election offices are unable to implement MFA because of outdated legacy systems and lack of vendor support. EI-ISAC should work with state and local offices to understand the full scope of the challenge and coordinate with a commercial provider to offer a managed solution for local offices to implement MFA on general office systems. In providing this service, EI-ISAC should offer technical support and resources for MFA implementation in existing election legacy systems. In addition, EI-ISAC should partner with common election system vendors to make it easier to implement MFA, as well as encourage

these vendors to implement MFA themselves. Election-specific systems may be harder to include in this effort because of strict requirements around certification and implementation.

Mandate reporting of election cyber incidents to CISA and the FBI.

Improved and increased information sharing regarding election cyber incidents was an incredibly important development for the protection of the 2020 election. Federal, state and local officials worked together to understand possible incidents and support response efforts in unprecedented ways. Moving from distrust seeded by the fallout of the 2016 election to this level of partnership is a tribute to the professionalism and commitment of state and local officials.

Building on this progress, Congress should require state and local election offices and private sector election providers to report cyber incidents to CISA and the FBI. This is a necessary step for two main reasons. First, CISA and the FBI have no ability to mandate this type of reporting themselves. While the vast majority of possible incidents in 2018 and 2020 were shared with the federal government, some were not shared with either the federal government or state officials. Time is of the essence during any cyber incident, but even more so with elections as officials work against a hard deadline and with limited resources. Required reporting will ensure timely and coordinated response from all levels. Second, given the sophisticated and persistent nature of the threats against elections, ensuring the federal government has a full picture of the activity out in the field is critical to providing a whole-of-government response to officials. The full capability of the federal government can only be brought to bear to protect election systems when the agencies charged with support of their defense have full visibility into the tactics, techniques and indicators of compromise employed by adversaries.

Establish minimum cybersecurity baselines for state and local election offices and election vendors.

In July 2021, the White House issued a “Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.” The memo pushes federal agencies to work more collaboratively with private sector companies that own and operate critical infrastructure systems to advance basic cyber practices. The memo requires agencies and the private sector to jointly establish voluntary guidance for the cybersecurity of critical infrastructure systems.

CISA, the Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC) should work together to publish a set of minimum cybersecurity practices that all election offices and companies should adopt. These practices should recognize that the majority of U.S. election jurisdictions are mid-sized to small counties, cities and townships that lack sufficient funding or IT support. We recommend starting with the NIST cybersecurity framework and adding or emphasizing the following:

1. **Create and maintain an inventory of assets.** For many election offices, items like patch management and incident response are hindered by a lack of understanding of

what systems and software the office owns and operates. Election offices should create and maintain an enterprise-wide inventory list with up-to-date information on system type and version.

2. **Require Multi-factor Authentication:** All critical systems, including business systems like email and voter registration access portals, should require MFA for all users.

3. **Ensure Network Segmentation:** All local election networks should be properly segmented from each other and other county networks. Proper segmentation greatly reduces the ability for malicious actors to access or impact election networks after compromising another county department or system.

4. **Maintain Access Control:** All election-related systems should follow the rule of least privilege. This means that only those that need access to a system should be given access, and only the access they need to accomplish their work. This should be applied to vendors and staff alike.

5. **Utilize Patch Management:** Implementing a patch management program reduces the likelihood of an organization having a cybersecurity incident particularly as a result of commodity malware.

6. **Move to .gov:** All state and local election websites should be moved to a .gov domain name. This is important for both security and to help combat mis- and disinformation, as .gov domain names are recognized as trusted government websites. CISA is offering .gov domains for free and is scaling up support to help states and localities move their websites over.

Centralize election IT infrastructure at the state level.

With the passage of the Help America Vote Act (HAVA) in 2002, many states took on much more responsibility for election administration. HAVA's requirement for the creation of statewide voter registration databases and requirement for the establishment of a chief state election official gave election leadership to several states that previously had little or no role in the administration of elections. For many of these states, it forced a partnership between the state and localities that administered elections that never existed before. As states worked to implement HAVA, many experienced pushback, and even outright hostility, from localities that previously had sole responsibility for administering elections.

In time, local and state election offices have largely worked through those challenges and established defined roles and responsibilities for the administration of elections, including voter registration databases. Some states took full control, running top-down, statewide voter registration databases. Others left control largely in the hands of the localities, serving simply as an aggregator of data at the state level, running bottom-up registration databases. Still, others have a hybrid system with a mix of top-down and bottom-up characteristics. Over time, these lines were further blurred with states taking on additional responsibility for military and overseas voters, with many beginning to offer sample ballots, voter lookup tools and ballot tracking.

The 2016 election permanently changed the threat landscape for elections. Russia, a nation-state adversary, was able to research, remotely target and, in a small number of cases, access election systems. This change in threat level must be met with a change in governance structure at the state and local level. Since HAVA, states have proven themselves capable of supporting elections by handling more responsibility for the administration and corresponding infrastructure of elections. In most cases, compared to local governments, states possess significantly greater budgets, staff and capabilities to protect from, detect and recover from cyber attacks against election infrastructure. Recognizing this, we recommend the following steps.

1. **Move to top-down voter registration systems**: In many cases, the decentralized nature has served election administration well. It has created flexibility for local election officials to creatively solve challenges unique to their county or township. However, voter registration systems are among the areas of greatest risk, according to a risk assessment released by CISA in 2020. Bottom-up states in particular have an increased attack surface and more risk to manage.

   It is time for states to take on the full responsibility of HAVA and move to top-down voter registration systems. Local election offices should not be asked to bear the responsibility of managing and securing these increasingly complex and important election systems. This move will also free up much-needed resources for local election offices to spend on other areas of election security and administration. A move to top-down voter registration across all states also will create an opportunity for the community to work collaboratively with CISA to create guidelines and new methods for securing and auditing voter registration systems, something that is difficult to do now because of the diversity of systems and infrastructure among county systems.

2. **Provide state-managed email accounts:** Many cyber incidents begin through the compromise of a local email account that is used to compromise other systems. A substantial number of localities maintain their own email servers. In many cases, this results in the administration of an email server within the county, sometimes by the local election office itself. In other cases, the local election office is left without any email support and is forced to use its own email account, sometimes resulting in the use of personal email accounts. States should utilize existing infrastructure to offer local election offices their own email accounts through the state, including cloud-based email services that the state is already using for its own email systems. If state-managed email accounts can't be offered, states should offer localities access to Microsoft or Google cloud-based email services. Both of these companies have offered additional protections and default secure configurations to election customers, and would greatly lower local offices' risk profile.

3. **Broaden implementation of cyber navigator programs:** Following the 2016 election, state election officials and their IT leads quickly came together to evaluate risk, strategize on mitigations and assess next steps in better defending their infrastructure. As they secured their own systems, state IT leads knew that the greatest risk rested across the machines maintained by counties, townships and cities that are actually responsible for running elections. Most recognized that state-level investment in local support would be necessary to properly manage the new risk environment. To shore up capability gaps at the local level, Illinois implemented a program dubbed the "Cyber Navigator Program" that provided state-funded IT leads to help localities evaluate risk posture and implement a checklist of steps to improve security and resilience. Several states, including Florida and Minnesota, implemented similar programs. Iowa took a similar approach, partnering with state and county IT leads to help local auditors secure election systems. This included engagement with the Iowa National Guard as well as cross-county support to ensure lesser resourced auditors received services and support. Moving forward, more states should implement similar state-funded programs to ensure that all county election offices have consistent and reliable IT support before and during elections.

Support good-faith security research and vulnerability assessments.

Since the passage of HAVA and widespread adoption of electronic voting systems, security researchers from academia and industry have focused their attention on the vulnerabilities in those systems. The quality of the relationship between the research community and election community has ebbed and flowed from highly contentious to begrudging respect.

Following the 2020 election, as election officials and industry were besieged with claims of rigging and hacking, security researchers saw their work distorted in pursuit of untoward goals. In an effort to defend both their work and the security of the 2020 election, researchers spoke out with one voice, making clear that "[m]erely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome" and calling the claims "technically incoherent." There is an opportunity now for these two groups to find common ground and support each other in improving both the security of election systems and confidence in the process. This can be done in several ways:

Adopt Vulnerability Disclosure Policies (VDP).

A strengthened relationship between election administrators and security researchers should start with states opening to good faith research through further adoption of vulnerability disclosure policies (VDP). These policies provide a safe haven for security researchers to find vulnerabilities in public-facing election systems and report them to the state election office for remediation. The Ohio Secretary of State's office was the first election office to implement VDP, with Iowa following closely behind. Other states have since announced their intention to implement a VDP. In addition, some of the largest voting system providers have announced creation of their own VDP, with four of the largest vendors currently offering VDPs. In 2020, CISA released a "Guide to Vulnerability Reporting For America's Election Administrators" that focuses on empowering election officials to create and implement their own VDP programs. VDPs not only build a bridge between the two communities, but also provide under-resourced election offices access to top-level security assessments at essentially no charge.

Moving forward, all 50 states and election technology providers should implement VDPs for their organizations. The VDPss should follow industry standard practices and include legal safe harbor to authorize testing and protect researchers. States should also consider requiring election system providers to have an existing VDP in order to be eligible to receive contracts. In addition, EI-ISAC should work with its executive board to create and implement a VDP that allows researchers to report vulnerabilities in local election infrastructure to the EI-ISAC, which would then notify the appropriate vendor or office. In serving in this role, EI-ISAC should work with the local election offices to determine the validity and severity of a report, as well as possible mitigation strategies. EI-ISAC should commit to collecting and reporting on the amount and types of vulnerabilities reported, and work with CISA to publish guidance on remediation of the most common vulnerabilities.

Expand open-ended vulnerability assessments.

Starting in 2019, CISA began offering election system providers access to Critical Product Evaluations. These are open-ended vulnerability assessments of the submitted system that is part of critical infrastructure. Testers tear apart systems looking for hardware, firmware and software vulnerabilities, issuing a report when finished of the discovered vulnerabilities and their severity. This type of open-ended vulnerability assessment has been discussed for decades, but has never taken hold in part because the federal testing and certification process is not properly structured for it.

In the aftermath of the 2016 election, DEF CON, the world’s largest hacking conference, created a Voting Village, self-described as “an open forum to identify vulnerabilities within U.S. election infrastructure and to consider mitigations to mitigate these vulnerabilities.” The Voting Village has exposed a broader range of security experts to the inner workings of election systems and brought election officials into the room with those experts to understand the mindset of a hacker. The village has also elevated election system security as the national security issue that it is. However, since its inception, the Voting Village has been controversial with some within the election community because of its unwillingness to provide context around the procedural controls that exist in elections. In addition, some organizers of the Voting Village openly mocked election officials, going so far as to describe them as “f---ing luddites.”

Bridging the gap between election officials and the security community through open vulnerability assessments is critical to continuously improving the security of elections. Doing so will increase the number of third-party experts available with exposure to election systems, allowing them to credibly affirm and amplify election officials' debunking of false claims made regarding the security of the systems.

Moving forward, the following steps should be taken to increase the exposure of election systems to third-party security research.

1. **Expansion by CISA of the Critical Product Evaluation Program**. For many vendors, this is an important introduction to open-ended vulnerability assessments and allows the vendor to understand the level of effort needed to mitigate vulnerabilities found during open-ended testing. CISA had robust participation in the evaluation program throughout 2019 and 2020 with many of the largest voting system companies participating. However, due to interest from other areas of critical infrastructure and limited capacity, CISA could not evaluate every system that was requested to go through the program. CISA should prioritize resourcing to allow any election system provider to submit its system to the program and receive an evaluation prior to the 2024 election cycle. In addition, CISA should continue outreach to private sector election system providers to increase the diversity of the types of systems submitted, including voter registration providers, election night reporting providers and electronic pollbooks. While these evaluations are useful for vendors themselves, making these evaluations public after sufficient review would significantly improve awareness of potential product security concerns for election officials looking to make acquisitions.

2. **Private sector participation in the DEF CON Voting Village.** The Voting Village has served an important role highlighting the national security importance of election systems. The Voting Village is an important forum for voting technology companies and election officials to engage with the security research community, but its value is currently limited because of the lack of new systems made available at the conference. Moving forward, the Voting Village should work more collaboratively with industry and election officials to secure relevant election systems for the conference. This will likely mean establishing protocols for the village to include vendor participation and responsible disclosure processes when vulnerabilities are discovered. This is typical across many of the villages at DEF CON, including the Aerospace and Healthcare villages. For their part, election technology providers should recognize the value that DEF CON participants can bring to evaluating systems, particularly for systems in development, and actively participate in the village instead of shunning it as unproductive.

3. **Incorporation of vulnerability assessments into the federal certification process**. Whether vulnerabilities are discovered during CISA's Critical Product Evaluation, at the DEF CON Voting Village, or through other channels, the ability for the federal certification process to intake those vulnerabilities and work collaboratively to respond to them is critical to deploying mitigations in the field. Currently, the EAC has no formal mechanism to intake reporting from independent third parties regarding voting system vulnerabilities. This leaves the EAC in the dark and unable to respond to discovered vulnerabilities. The certification program must create a process by which it intakes vulnerability reporting for certified systems and works with vendors and election officials to respond. In addition, the certification program must reform its standards development process to nimbly incorporate vulnerability reporting into the feedback loop in order to inform revisions to the VVSG.

4. **Eliminate legal barriers to security research.** Too often, especially in the elections space, security researchers are deterred from testing for or disclosing vulnerabilities due to fear of legal action. Specifically, Section 1201 of the Digital Millennium Copyright Act (DMCA) and the Computer Fraud and Abuse Act present legal risk for security researchers. While the U.S. Copyright Office has added security research exemptions via the triennial rulemaking process, the exemptions are too narrow and only temporary. Congress should codify strong security research exemptions for the DMCA into law. Further, Congress should explore similar security research exemptions for the Computer Fraud and Abuse Act, contingent on a good-faith, harm-minimizing research approach and researchers making an attempt to disclose any discovered vulnerabilities.

Conclusion

While the progress made in the four years between presidential elections was immense, it was only a beginning. Following the 2020 election, much of election official's energy and attention has turned to responding to mis- and disinformation. This is understandable given the scope and volume of mis- and disinformation they faced throughout 2020 and since, but could result in underappreciating the resources or attention necessary to improve the security of their systems. In an environment where the loser of an election may not accept the result no matter the margin of victory, the ability to show the resilience and security of the process is more critical than ever. Continuously improving security measures, alongside better tools to fight mis- and disinformation as it arises, are the keys to building confidence in future elections.

For the foreseeable future, election administrators will be in the spotlight, forced to deal with advanced and persistent cyber threats, as well as physical threats of violence driven by mis- and disinformation targeting our democracy. The spotlight is bright and unrelenting, and more must be done to empower election officials with the tools to deal with it. The alternative is a world in which the hard-won progress of the security and accessibility of our elections is a casualty of a caustic political environment driven by greed and a thirst for power rather than the higher ideals of our democracy.