Stanford | Internet Observatory
Cyber Policy Center

Testimony of Matthew Masterson
Non-Resident Fellow
Stanford University Internet Observatory
U.S. Senate Committee on Rules and Administration
"Emerging Threats to Election Administration"
October 26, 2021

Chairwoman Klobuchar, Ranking Member Blunt, and members of the Committee,

My name is Matthew Masterson. I am a non-resident fellow at the Stanford Internet Observatory (SIO) where my work focuses on mis- and disinformation and election security. The Stanford Internet Observatory is a cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, with a focus on social media. Prior to SIO, I led the election security work at the Cybersecurity and Infrastructure Security Agency (CISA) from 2018 through the 2020 election. I appreciate this opportunity to appear before you today to discuss the ongoing and pervasive threats targeting election officials, workers and private sector employees who support elections, and the steps we can take to better protect those essential guardians of our democracy.

Myself and a team of SIO students recently released two reports focused on the 2020 election and threats to American democracy. The first, is an oral history of the 2020 election from the perspective of the federal, state and local election officials who defended it. The second is a policy paper that builds off of what we heard throughout the interviews with the elections officials regarding the threats they are facing and recommendations for how to respond to those threats.

Election officials are rarely in the spotlight. They toil day after day, hour after hour in preparation for the times, every year, when their voters head to the polls — or their mailboxes — to cast their votes and have their voices heard. Election officials know they have done their job well when, in the aftermath of each election, no one knows their names.

The 2020 election placed them at the center of national attention in a way not seen in decades — if ever. A global pandemic brought the systems and people that run elections to the brink. In the face of unprecedented challenges, election administrators buckled down and worked with their communities to keep voters — and their votes — safe. Record turnout and a smooth election day validated election officials' incredible work and commitment to risking their own health and safety to get this monumental challenge done.

The reward for their professionalism and bravery? A massive mis- and disinformation campaign targeting the integrity of the election and those who administered it. Following election day, narrative after bad-faith narrative took aim at election officials, often culminating in months of personal threats against their lives and the lives of their family members.

As the bipartisan Florida Supervisors of Elections recently wrote in a memo, "During and after the 2020 Presidential Election, the integrity of our democracy has been challenged by misinformation, disinformation and malinformation that sows discord and undermines trust in America's electoral process. Many of us have been threatened by our fellow citizens who have been led astray by these deceptions." These threats have targeted officials from across the country and of both parties. They have been directed at statewide elected officials, local county, city and township officials, private sector employees and even poll workers.

Threats to Election Processes

While many threats to the election process exist, three stand out as especially concerning for the 2022 election and beyond.

1. **Election officials' capacity to do their jobs in their communities is degraded by physical threats and broad distrust fomented by mis- and disinformation.**

   Election officials are more physically threatened than ever before. From our interviews, recent government reports, and non-profit and academic research, it is clear that state and local election officials face increasing threats to their physical well-being and that of their families. The perpetrators of these threats are fueled by online conspiracies that cast election officials as malicious actors bent on meddling in election results. Innocuous glitches and quickly corrected human errors have been stitched together to fit broad conspiratorial narratives as alternative explanations for election results.

   These conspiracies, and the threats behind them, make treacherous a fundamental tenet of serving as an election official: the ability to work within the community to determine the safest and most effective way to run each election in that locality. This loss of connection with the community has very real consequences. We run elections at the local level so citizens can engage directly with the process and those who run it. Loss of that connection due to legitimate concerns for the safety of election officials and their employees, means less questions answered, less enhancements to access and security of the process based on voter experience and in the end less trust of the process and those who run it.

   As threats continue, physical security assurances will become increasingly critical. Even if additional protection is provided to those who are threatened, many election officials may face the horrible choice of either continuing to receive threats for doing their jobs, or leaving the profession. The field is already losing election officials at an alarming pace. The loss of experienced election professionals could open the door to more politically motivated and less experienced actors pursuing those vacant positions, further weakening our democracy.

2. **The playbook for undermining confidence in election results is well-defined and available for foreign and domestic influence agents.**

In a series of press releases leading up to the 2020 election, the FBI and CISA released an unprecedented public warning that America's adversaries would use social media posts questioning election process changes to undermine confidence in election results. This warning turned out to be prescient, as Iranian operatives posed as members of the Proud Boys to intimidate voters and use hacked voter information to insinuate election systems were not secure.

Despite foreign efforts to crater confidence in the security of the vote, it is domestic actors that most furthered the mission, providing fertile ground for adversaries to undermine confidence in future elections. While turnout in the 2020 general election was historically high, Americans' trust in the freedom and fairness of their elections polarized quickly after 2020, more so than in previous elections. Moving forward, we should expect nation-state and domestic actors to build off this playbook, creating more sophisticated and targeted messaging aimed at denigrating trust in elections.

Assailants of election confidence and democracy are emboldened and active across a variety of platforms, while defenders of civic integrity remain disparate and at times disjointed. Local election offices, the most under-resourced defenders of all, are on the front lines of fighting these viral falsehoods targeting elections. This dynamic is untenable. A county clerk should not be expected to monitor social media platforms for falsehoods, analyze for scope, scale and themes, and respond to each one. Many stakeholders are on the defensive side of civic integrity, including state election offices, federal partners, social media platforms, academia and non-profits that can support local election officials. Presently, these disparate groups are poorly funded or insufficiently coordinated on local support. If defense against the anti-election confidence playbook is to succeed, this gap must be filled by a well-organized and unified response.

3. Inconsistent funding and lack of governance structures around elections IT continue to perpetuate vulnerabilities.

The cyber threat landscape faced by state and local election offices has progressed significantly since the 2016 election, which was the first time an adversary of the United States targeted American democracy in such a brazen way. Since, there has been a concerted effort at all levels of government to connect state and local officials to cybersecurity experts and each other, as well as to develop best practices. Due likely in part to increased awareness of and preparation for cyber threats to election processes, the 2020 general election did not experience a significant cyber event that prevented citizens from voting or that impacted the tally of votes.

Despite 2020's success on the cybersecurity front, there was a continuous increase in cyber threats to election systems and state and local IT systems generally. Ransomware

attacks often target these jurisdictions because of lax cybersecurity measures and a relative lack of defensive resources, causing ransomware to be one of the largest threats to government IT security writ large, including for election systems. A ransomware incident can shut down a local government office for weeks or months, wasting valuable technical resources to undo what is generally preventable damage. Election systems become more attractive ransomware targets for criminals before and during an election because the operational constraints of running an election may make officials more likely to pay ransoms. Additionally, low-hanging vulnerabilities such as insecure databases and other public-facing website configuration vulnerabilities are exploitable by ideologically motivated adversaries and financially motivated criminals. Well- resourced adversaries did not wreak havoc during the 2020 election, but may try to in the future. That innocuous hiccups in election systems can feed such pervasive conspiracies significantly increases the negative impact of even minor, reversible incidents targeting non-critical election systems, such as unofficial results reporting.

While progress has been made in coordinating against cyber threats to election infrastructure, local IT professionals in county, city and township offices around the country remain understaffed and under-resourced. Incremental election security funding has been provided to state and local election entities for election security improvement, but many meaningful upgrades would require consistent funding from all levels of government to implement and maintain. Additionally, some local offices still do not have dedicated IT staff, and many use legacy equipment that is exploitable by adversaries. In the end, the asymmetry of cybersecurity means that threat actors still possess a high tactical advantage against beleaguered defenders due to the distribution of IT management across levels of government.

In light of the aforementioned threats, and others yet to come, I would propose 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. For most election offices, predictable funding is easier to manage and implement than the Help America Vote Act (HAVA) model of a one-time massive dump of money into the system. This is because state and local contracting rules and regulations require time for acquisition and implementation. Contracts for threat intelligence sharing, cybersecurity monitoring and the hiring of IT personnel are often paid over time instead of in one single payment, giving the appearance of a lack of spending by jurisdictions as opposed to strategic spending over time to maintain support and capability. The HAVA funding model incentivizes large purchases of infrastructure in tight timeframes, which led to demonstrably poor purchasing decisions from several state and local officials. For instance, in the rush to use funding to implement statewide voter registration databases after HAVA was passed, many states simply contracted with vendors for rapid development and deployment of these databases without the usual requirements or even, in some cases, a competitive bid process. This led to states upgrading or piecing together a commercial and internally developed system within years of initial deployment because the newly acquired systems were unable to meet the developing needs of the office.

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, if any, 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. We recommend 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.

Continue to Improve the Cyber Resilience of American Elections

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, 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. The most effective type are risk-limiting audits (RLAs), which allow a jurisdiction to assess the results of the election to a certain level of statistical confidence. RLAs can often have the added benefit of needing to audit fewer ballots than fixed percentage audits (e.g., 2% of votes cast in the county) while increasing the confidence in the accuracy of the result.

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.

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

Following the 2016 election, the greatest area of frustration for state and local election officials was the lack of coordination from the federal government. Many officials felt the federal government had hung them out to dry by not providing enough information or details regarding the Russian activity and how to respond. In some cases, states where cyber incidents occurred had to wait for years to be fully briefed on what happened. The FBI and CISA recognized their shortcomings from 2016 and changed their respective incident notification policies. Both FBI and CISA now notify chief state election officials when a cyber incident occurs in a locality in

their state. This is a dramatic change from prior practice, in which only victims received notification, and was an important step to ensuring a coordinated and comprehensive response to any election-related cyber incidents.

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. Congress is already considering broader legislation on cyber incident reporting, and this requirement for the election sector is consistent with the intent of those bills. This is a necessary step for two main reasons. First, CISA and 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 the Cybersecurity for Critical Infrastructure Control Systems." The purpose of the memo is to push executive branch agencies to work more collaboratively with private sector companies that own and operate critical infrastructure systems to advance basic cyber practices. The memo requires these agencies to work jointly with these companies to 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 minimum set of cybersecurity practices that all election offices and companies can 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.

Conclusion

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, but could result in underappreciating the resources or attention necessary to improve the security of their systems. 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.

Our elections are imperfect; they are massive, messy, under-funded and under-resourced. But they are accurate, secure, accessible and fair because of the tireless work of state and local election officials. 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. We must fund elections from the federal, state and local level on an ongoing basis like the national security issue they are. The only response to this sustained attack on our democracy is a sustained investment in protecting it.