Written Testimony

of

Noah Praetz

Former Director of Elections

Office of Cook County Clerk

before the

United States House Committee on Homeland Security

Regarding

"Defending Our Democracy: Building Partnerships to Protect America's Elections,"

February 12, 2019

Washington DC

Biography

Noah Praetz was the Director of Elections working under Cook County Clerk David Orr and then under Clerk Karen A. Yarbrough. He was responsible for the overall management of elections in Cook County, Illinois, one of the largest jurisdictions in the country serving 1.6 million voters.

He started as temporary worker hired to do data entry prior to the 2000 presidential election. In 2007 he became Deputy Director and in 2013 he was appointed Director.

Mr. Praetz currently runs an elections consulting practice. He teaches election law at DePaul University College of law. He is an advisory board member at the University of Chicago's Cyber Initiative.

Mr. Praetz was on the executive committee of the Government Coordinating Council representing the local election officials as Homeland Security sought guidance on how best to support the Election Community. He was the Treasurer of the International Association of Government Officials. He was also co-chair of the Election Center Cyber Security Committee. He was active in the Illinois Association of County Clerks and Recorders. He has presented on Election Security, Sustainability, Election Day Management, Online Registration, Voter Registration Modernization and other Election Related items.

Executive Summary

Election Officials have been securing our nation's votes and voter records for a very long time. We have been securing digital infrastructure for a more than a decade. But the changed environment and the expectation of continued sophisticated attacks forces them to up their game.

Spurred by the need to defend against foreign enemies, Federal and State officials have been working successfully to find a good balance of federal involvement in elections, without trampling on authority that the states zealously guard. Good progress is being made.

However, even as the community of election officials appreciate that election 2018 was free of any known incidents, they largely recognize that those successes are probably less a function of their efforts than they are a function of our nations adversaries' probable choice to hold back. The fundamentals of election security, and the investments neeeded to ensure improved security, have not changed since the summer of 2016.

Broadly, the fundamentals are these, local election officials are the ones who control, secure, and run elections. Locals - 108 in Illinois and over 8,000 nationwide - are on the front lines of this new battlefield. Locals control almost the entire election infrastructure. Locals are the entities most in need of support and attention. Locals need help to fortify themselves, and our most important institution, against the high probability threat actors they've been warned of. The States, with partnership from the federal government, are the entities that are now, and will continue to be, the leaders needed to support the security efforts to the local election officials.

While in Cook County we studied and undertook significant efforts at securing the infrastructure and helping raise awareness within the ecosystem. We concluded that to decrease the likelihood of successful attack on digital services, each local election official must have ready access to a savvy dedicated partner - an election infrastructure security officer. Most locals don't have that capacity today.

Local election officials cannot master this problem without direct support of skilled experts. We suggested this be handled by a brigade of digital defenders, or what the government coordinating council calls "cyber navigators," supporting local election officials into the future.

These "navigators" should adopt the mantra of Defend, Detect, Recover. They need to accomplish these three vital goals. They can help improve defenses within election offices, following the specific recommendations of Center for Internet Security or Defending Digital Democracy -- we believe they'll quickly bring up the floor of the elections security ecosystem. They'll also establish detection techniques. And they'll develop recovery plans for when attackers penetrate the first and second line.

To accomplish this, the "Navigators" will secure free support on offer from public and private organizations, like Homeland Security, state governments, and companies like Google and Cloudflare. They will also work with outside vendors who provide much of the elections infrastructure and support to local officials. Third, they will build a culture of security that can adapt to evolving threats through training and constant re-assessment.

Voters should feel confident that we have resilient election systems, with paper ballots and good audits almost everywhere. But voters should also understand that without continued investment in people and products the possibility of a successful attack increases. As does the likelihood that losing campaigns may cultivate cynicism about the integrity of our elections for their own purposes. Democracy is not perfect. As Churchill said, it is the worst form of government except for all the others. We need to protect it. We will regret it if our democracy is damaged because we looked away at a critical moment.

TESTIMONY

Thank you, Chairman Thompson and Ranking Member Rogers, as well as all members. It is an honor to be here. I am reminded as an election administrator that when we certify results we are an essential part of the process that bestows not just power, but legitimacy. And that legitimacy attaches because of the essential American belief that our elections reflect a trusted and true accounting of each election. I speak to you today in support of efforts to ensure that legitimacy remains the key virtue in our elections.

My name is Noah Praetz. Two weeks agao I stepped down as Director of Elections in Cook County Illinois where I worked for Cook County Clerk David Orr, and recently Clerk Karen Yarbrough. I began my career in 2000 and during that time our office tried to lead on technology and security - using applied forensics in elections; creating widely circulated cyber-security checklists in advance of the 2016 elections; and publishing the first white paper written by election officials in the wake of the 2016 attacks. Recently, I helped the Center for Internet Security (CIS) adapt their digital security expertise to the unique context of elections and also spent a little time talking to the Defending Digital Democracy program at Harvard's Belfer Center (DDD). As co-chair of the Government Coordinating Council (GCC) that the Department of Homeland Security created to help address election security, I worked with federal, state and local leaders in elections, technology, intelligence and law enforcement.

In the past 18 months I have testified before the United States Senate Rules and Administration committee once. On two occasions I testified before the United States Election Assistance Commission (EAC) and on two occasions I testified before Illinois legislative committees. I have presented before the numerous meetings of election officials from Illinois and from around the country. Every time, I strive to deliver the same message:

- The threats to election infrastructure are real.
- Elections are largely run and secured locally, so security efforts, let by the states and augmented by the federal government, need to be concentrated locally.

As election officials, we must accept the conclusion of the intelligence community - our elections were attacked and are vulnerable. And while enemy hostile probes of our news and influence systems appear to have been more successful than those on election administration, we have to expect the attacks will evolve. We, as election administrators, must defend our section of the line – by securing all elements of our voting infrastructure.

Cyber-Security – One More Sword to Juggle

Prior to 2000, election administrators served mostly as wedding planners, making sure the right list of people came together in the right place with the right stuff. After *Bush v. Gore*, the Help America Vote Act (HAVA) heralded in new era of voting technology, and we became legal compliance and IT managers. We've been working to protect digital technology since then. But the 2016 election showed irrefutably that sophisticated attacks are to be expected and that we must also be cyber-security managers

Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees, this threat applies to both preliminary returns announced on election night and to official, final results. Beyond corrupting election results, the threat also reaches the large variety of systems used to run seamless elections.

Therefore, the new security mantra, or security framework, for local election officials must be "defend, detect, recover."

Security isn't just about defense. Perfect defense is difficult or even impossible. I could cite a list of our best companies and government entities that have been breached despite significant defensive investments. Instead, the challenge of security is to ensure no attack exceeds our resilience–our ability to detect and recover–whether that requires restoring lost data or even recounting ballots - to establish election results that are trusted and true.

Because state laws vary, local election officials confront a different security matrix in each state, affecting their ability to defend, detect and/or recover. States with great audits (detection) and paper ballots (recovery) are much more resilient by definition; and the burden of defending their voting system perfectly is consequently much lower. On the other hand, states without great audits and without paper ballots place the unenviable burden of perfect defense on their local election administrators.

In 2017, Cook County Clerk David Orr and I published a White Paper called "2020 Vision: Election Security in the Age of Committed Foreign Threats." It is included at the back of this testimony. But I want to acknowledge that different bodies of this congress have already taken action that broadly agrees with our vision and I commend that work.

Elections are Secured Locally

I have tremendous appreciation and respect for state election officials and their responsibilities and efforts. They are often the mouthpiece of our institution and responsible for managing the regulatory framework. For the past 16 years many have also managed their state's voter registration systems. In some states they take a far more active role in protecting other parts of the infrastructure. And it was states that were the named targets in 2016. But let there be no mistake - local election officials are on the front lines of this new battle field: 108 in Illinois and over 8,000 nationally. So, by and large, local election officials secure the nation's election infrastructure. Locals install, store, monitor, test, deploy, run and audit the voting machines and software. Locals install, store, monitor, test, deploy, run and audit the electronic pollbooks. It is locals who manage warehouses, informational websites, voter databases, polling places, GIS Systems, results reporting systems, military voting systems, command centers and the myriad digital services we rely upon in modern American elections. It is a local job to defend these systems, to institute controls that would detect breach, and to deploy mitigation strategies that can guarantee election processes and results that are trusted and true. It is there job to ensure recovery.

Most of us are county officers, and we are facing down powerful, shadowy adversaries, like Andy of Mayberry sent to repel an invading army. We need advice, support, and resources – first, for better technology and routine hand counted audits which can give additional confidence that digital results are accurate. Second, and most critically today, we have a pressing need for top-notch personnel with the skills to navigate the current cyber battlefield. Our country's local election officials need direct human support as we work to defend ourselves against the onslaught of digital threats we've been warned about.

Cook County Efforts

Since the summer of 2016 we stepped up our efforts to protect ourselves and to protect the broader ecosystem: We introduced additional hand-counted audits to our state-mandated five percent machine re-tabulation. And we are pushing state legislation to add additional audits to election results – in the form of Risk Limiting Audits.

We did a complete mapping of all our systems and conducted a point analysis of potential vulnerabilities. We have documented all defensive measures employed and created a list of those we hope to employ going forward. We also documented all methods of detecting breach, as well as those we hope to

employ in the future. Finally, we are developing our recovery plans for any breach at any point on any system. Before November of this year, we will practice every recovery method.

We began installing new election equipment that will be easier to defend and will make detection and recovery significantly easier.

We introduced state legislation to help local election officials bring in more expertise and cyber monitoring capability.

We worked to create a communication structure in Illinois with federal, state and local cyber experts, technology experts, law enforcement officials and election officials.

We teamed with our neighbors at the Chicago Board of Elections to hire an election infrastructure and information security officer.

We worked with MS-ISAC to get rapid intelligence on vulnerabilities and specific threat information to our networks. And we have pushed our colleagues around the state to join it and the elections ISAC. Additionally, we have gotten threat briefings from DHS and FBI.

We worked with DHS to conduct cyber scans of our websites - and to run a full risk and vulnerability assessment. And let me say that I am glad the folks working for homeland security are on our team. I firmly believe if every election official, state or local, undertook a similar effort, there would be a deafening roar from my colleagues for more resources to procure modern technology and institute modern controls.

We worked with the folks at DEFCON on some of their activities related to training election officials on the defense of networks.

I co-chaired the newly created Government Coordinating Council (GCC) set up with DHS to help drive federal policy and resource allocation. I sit alongside the Chairman of the Election Assistance Commission (EAC), the President of the National Association of Secretaries of State (NASS), the President of the National Association of State Election Directors (NASED), and from DHS Deputy Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate (NPPD). In that roll I tried to continually push for the advancement of local official's concerns.

In all efforts we learned that coordinating efforts is critical to our individual and ecosystem success.

Coordinated Efforts

There has been a tremendous amount of attention on the states, and their relationship to the federal government and it's great to see that relationship mending and great information starting to be shared between the two groups. On the GCC we have worked hard to refine a plan for securing our sector as well as protocols for sharing information throughout the ecosystem. We are working with the private sector vendor community to ensure we have a common approach to protecting the sector.

Federal government agencies now know how to communicate to the state level election professionals and vice versa. What remains unfulfilled is the assurance that the information can get all the way down to the local level and that the locals are prepared to digest the information and take necessary action.

It is time to ensure that the successful effort to normalize relations with state officials be duplicated with local election officials. Like an iceberg, the mass, and indeed most of the risks to the nation's election infrastructure, lies below the surface. And its security lies in the hands of women and men who run elections at the local level.

Given concerns with federalism, the most likely path for successfully fortifying local election officials is through state government and state election officials. But it's important that they envision their job as helping

ensure locals are resourced appropriately and meeting important security metrics. I have no doubt that our state officials are up for the challenge and I look forward to assisting our industry mature in this direction quickly.

Increased Stable Investment & Short Term Spending

We have looked to our state and federal funders and regulators to fortify locals on this battlefield. Given the costs of regular technology refreshes and support for human resources with cyber capacity, the needed investment is very large. And locals need a signal that they can invest now for security and not squirrel away recent money for some future episode.

Nevertheless, the recent investment is greatly appreciated. Congress just released $380 million to combat the election cyber security threat. And that is an important start. It may be necessary for the states, federal government and locals to collectively invest that much annually. Meanwhile, Americans justly concerned about the costs need confidence this money will be spent well. In my mind there are two top priorities. First, a handful of states and counties still have paperless voting systems. These should be replaced as soon as possible.

Second, everywhere, we must improve the security capacities of local election offices. Most are run by a just handful of incredibly dedicated and hardworking heroes. But a handful of people making critical security decisions are outmatched against the threats we've been warned of.

In a local newspaper last year we called for a brigade of digital defenders to be deployed to serve election offices around Illinois and the nation, starting now and working through the 2020 presidential election and beyond. Recently, the Government Coordinating Council, comprised of the leadership of America's election organizations, suggested a similar construct, suggesting that states employ "cyber navigators" to help fortify local election officials.

Illinois Approach

In Illinois we formulated a loose security group consisting of representatives of Homeland Security, FBI, the Illinois State Police and their Cyber Team, Illinois Information Security Office, the leadership of the local election official associations, and the State Board of Elections. Originally our some of local officials and the State Board of Elections had desired to pass through the HAVA funds to the local election officials based largely upon voting age population. But as our group and state legislators digested the cyber security problem, we recognized that such a distribution would not be effective in fortifying most of the locals. First, regardless of the number of voters served, all 108 election officials had nearly identical cyber footprint, in that they had the same number of networked-attached digitally exposed systems. Second, the larger offices already had some capacity to tackle this problem – whereas the smaller offices are squeezed so tightly they can barely comply with the current requirements, let alone secure the entire elections threat surface area.

After the GCC issued guidance suggesting "Cyber Navigators", the state legislature mandated that at least one-half of the HAVA funds just released be expended on a "Cyber Navigator" program to be administered by the State Board of Elections. The State Board is likely to get help fulfilling this mandate from other organizations with cyber expertise. By and large, local election officials supported the bill. And our state board is eminently capable of fulfilling the mandate.

These "Navigators" need to accomplish three vital goals. First, they should work to institute the election security framework – defend, detect, recover. They can help improve defenses within election offices, following the specific recommendations of CIS. We believe they'll quickly bring up the floor of the elections security ecosystem. Appropriately supported, we can see massive improvement very quickly. There is low

hanging fruit, but even low hanging fruit needs to be plucked. They'll also work to support locals' efforts at instituting detection techniques and recovery plans. Second, the "Navigators" will do the work necessary to secure the free support being offered by public and private organizations, like the Department of Homeland Security, state resources, Google and Cloudflare, or the Elections Information Sharing & Analysis Center; they will also work with the outside vendors who provide much of the elections infrastructure and support to local officials. More importantly, they will help build a culture of security that adapts to the evolving threats we face through training and constant assessment efforts. Illinois' 108 local election offices will mature quickly with this reinforcement. As specific mitigations and upgrades are identified by Navigators, the State Board should be positioned to quickly provide that investment.

It is expected that the State Board of Elections will take some small portion of the remainder of the HAVA funds to support their own infrastructure, naturally, since they manage and maintain the statewide voter database. Everything else shall be distributed to the local election officials to invest as they see fit, subject to the guidelines. I'll note that our legislature sought to compel participation in the Navigator program by making receipt of future grants contingent upon local official participation.

In Illinois, we recognized that this is inherently a local problem. But we also recognize that locals cannot solve this problem themselves. This coordinated, managed approach assures appropriate assessment and remediation efforts can be efficiently implemented. We are utilizing existing expertise from other areas of federal, state and local government as force multipliers. And we are excited that our State Board of Elections is taking on this new mandate and moving quickly to implement it.

This massive reinforcement effort can be accomplished here and nationwide. And it can be done now. It will require the states to cut through the red-tape that can delay action. This may mean relying on existing contracts, or even emergency procurements. But states must do whatever they need to do to get the army of "Navigators" on the ground this summer. After all, the danger is not hypothetical. We're bracing against the renewed attacks we've been told to expect.

Supporting a Resilient Public

One job of an election administrator is to conduct elections so that losing candidates accept the fact that they lost fairly. Anything that hinders our ability to do that decreases confidence in the system. And undermines our ability to bestow legitimacy – not just victory.

Election officials deploy a variety of networked connected digital services, such as voter registration systems, and unofficial election results displays. Each of these is a ripe target for our adversaries. A successful attack against those services may not change a single vote, but could still damage public confidence. This is particularly true in a time of great public suspicion, exacerbated by a disappointing proliferation of gracelessness and grandstanding.

Our public confidence is already weaker than it should be. Vacillating voting rights rules, no matter how marginal the effect, are disconcerting to many people, naturally suspect given our history. Additionally, some media, activist groups and politicians have acted in ways that ultimately prey on Americans' insecurities about their most cherished institution, either through outlandish claims of fraud, or overstated claims of suppression. Such actions have done a disservice to the institution we serve and consequently to our ability to bestow not just victory, but legitimacy. We must be very careful to calculate not just the relative effects on power that election rule changes can have, but also the relative effects on legitimacy. Or put another way – will losers be more or less likely to accept that they lost fairly.

Some losing candidates are already apt to call their defeats into doubt. A new digital breach - no matter how far removed from the vote counting system - could turn sore losers to cynicism, disbelief, even revolt. That's the reaction the enemies of the United States want.

In fact, in the face of direct targeting of a state or local election office it is very possible that there will be some service disruptions – most likely to the network connected digital services like election results websites.

The bottom line is we can't eliminate every chance of breach, but we can make sure that successful attacks rare. And we can provide assurances that we are prepared to recover quickly when they happen. We can do this with support at the local level. I support federal efforts like the Secure Elections Act. While I would always advocate for more local participation, in the current environment, doing something imperfect now is greatly superior to doing something perfect at some point in the future.

As Americans, we get to choose how we want to respond to potential disruptions. The damage of a foreign attack on our elections infrastructure will be greatly diminished if the targeted institution is also being supported internally with respect.

Thank you for the opportunity to appear today. I look forward to your questions.

White Paper

2020 Vision: Election Security in the Age of Committed Foreign Threats

Sponsored by: Cook County Clerk David Orr

Authored by: Noah Praetz, Director of Elections

December 2017

The entire national security establishment admonishes that threats to our election infrastructure are real. Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees this threat applies to both preliminary returns announced on election night and to official, final results.

Beyond results, the threat applies to the large variety of systems used to run seamless elections. These include electronic and paper pollbooks; voter registration and election management systems; websites with voter tools and public information; and a variety of other subsystems such as: GIS, ballot printing system, mail ballot preparation and processing system and a variety of essential election support systems like election day control centers.

Local election officials - nearly 9,000 of them in the country - are the shock troops on this new battlefield. They desperately need resources, including federal government resources.

Policymakers and funders must act now to ensure election security

The new security mantra for local election official's is "defend, detect, recover."

Perfect defense is difficult or even impossible. Instead the challenge of security is to ensure no attack exceeds our resilience–our ability to detect and recover–whether that means restoring lost data or even recounting ballots to establish election results that are trusted and true.

Each state has a varying security matrix to operate in; their mix of ability to defend, detect and recover. States with great audits (detect) and paper ballots (recover) are much more resilient by definition; and the burden of defending their voting system is consequently much lower. On the other hand, states without good audits and without paper ballots place the unenviable burden of perfect defense on their election administrators.

Below is a challenging, comprehensive, yet achievable list of actions to protect the integrity of these multiple systems. Make no mistake, this will be a painful and expensive undertaking. But the protection of our foundational institution requires this sacrifice.

Responsibilities of Policymakers and Funders:

Defend

Increase the defensive capacity of local and state election officials by:

1. Supporting a digital network for all local election officials that will facilitate rapid sharing of threats and incidents, as well as supporting increased training and resiliency;

2. Financing an Election Infrastructure and Information Security Officer (EIISO) (or consultant) servicing every local and state election official in the country;
3. Ensuring that threat and incident information known to Government is shared appropriately throughout the election ecosystem.

Detect

Increase the catastrophic breach detection capacity by incentivizing:

1. The use of modern public audits of all elections;
2. The use of modern voting technology that captures a digital image of each ballot that can be tied to the original ballot and the cast ballot record;
3. The use of monitoring sensors on the networks of all willing election officials.

Recover

Eliminate even the most remote possibility of an undetectable catastrophic breach by replacing all paperless voting systems that currently serve nearly 20 percent of the country.

Release election officials from their burden of being perfect every single time!

Potential Approach for Election Officials and Their Election Infrastructure and Information Security Officer:

Defend

- Get experts into the office. Engage outside cyber security resources & professionals. No election offices can handle this problem on their own. Inside most elections offices, there simply is not the complete capacity to accept the threat, assess the vulnerability, digest recommendations, manage mitigations and perfect recovery.
    - Utilize as many free local, state, and federal (DHS, CIS and MS-ISAC) tools as possible,
        - If government resources are unavailable, or underwhelming, hire private firms or partner with academic institutions.
    - Collaborate with resources inside local, state and federal government because we are not alone in facing this type of threat include the fusion centers.
    - Bring in outside resources to partner with information technology and information security teams, with a focus solely on election security.
        - The reality is that most election officials share their internal information technology and security resources with every other county office engaged in critical activities, such as health and public safety. It can be nearly impossible to get the attention necessary for election security unless it is the primary focus of those resources.
- Understand and limit the threat surface area; or all possible points of vulnerability for malicious attack.

- Inventory all election related systems: e.g. voting machine and vote counting system; e-pollbook system; voter registration / election management system; mail ballot delivery and processing system; and online-systems such-as voter registration, mail ballot request tools, voter information lookup;

- Map how systems work and data flows, and mark every single point of vulnerability;

- Limit the threat surface area by making policy decisions that reduce points of vulnerability wherever possible (this is about managing risk, not eliminating it.)

- Employ defense tactics and policies for each system – online or not;

  - Implement the Center for Internet Security's top 20 cyber controls. Do the top 5 first. These include:

    1. Inventory of Authorized and Unauthorized Devices; 2. Inventory of Authorized and Unauthorized Software; 3. Secure Configurations for Hardware and Software; 4. Continuous Vulnerability Assessment and Remediation; 5. Controlled Use of Administrative Privileges; 6. Maintenance, Monitoring, and Analysis of Audit Logs; 7. Email and Web Browser Protections; 8. Malware Defenses; 9. Limitation and Control of Network Ports; 10. Data Recovery Capability; 11. Secure Configurations for Network Devices; 12. Boundary Defense; 13. Data Protection; 14. Controlled Access Based on the Need to Know;15. Wireless Access Control; 16. Account Monitoring and Control; 17. Security Skills Assessment and Appropriate Training to Fill Gaps; 18. Application Software Security; 19. Incident Response and Management; 20. Penetration Tests and Red Team Exercises;

  - Employ election system-specific defense and detection tactics across specific systems;

    - These can include all the hardening options that systems may have, such as locks, seals, chain of custody, advanced authentication, etc.

Detect

- For each vulnerability point identified in the mapping process, consider a method of detecting whether something anomalous has happened; or brain storm the first place such an intrusion might be detectable.

- Validate everything; every available log should be checked including: seals, time sheets, cameras, swipe cards, login data, registration statistics, etc.

  - Behavioral analysis tools and procedures can and will point out what is going on. For example, voter registration follows a natural pattern year over year. Identifying the pattern and watching for anomalous behavior works.

- Use forensics when possible.

  - A forensics analysis of the software system employed can offer a high level of confidence that it is operating as certified. This is particularly true in the voting system environment. Comparing snapshots of deployed software with a clean reference copy during a live election is a powerful verification technique.

- Conduct public audits of the election results that allow for a visual comparison of the cast ballot record with the ballot itself.

    - Be transparent and brace for public scrutiny.

    - Crowdsourcing the election brings the greatest confidence, but also the greatest public scrutiny. "Sausage making" will be on full display. Consider publishing ballot images scrubbed of identifying marks. In the short run this can create volatility, and people may scrutinize the office and the software used, but ultimately the confidence levels will be increased.

    - Work to investigate audit styles that bring the highest level of confidence to the most stakeholders. Consider the use of sophisticated yet efficient testing algorithms, such as risk limiting audits.

Recover

- For each vulnerability point, assume a successful breach and determine how to recover.

- Where possible, make policy decisions and investments that yield the clearest path to recovery.

    - For example, on electronic voting machines: after removing paperless systems consider that, ballot marking devices are better than machines with paper audit trails. Digital scanning devices that create images of ballots are better than scanning devices that don't.

- Build in redundancy that doesn't rely on technology.

    - For example, paper pollbooks backup electronic pollbooks. Emergency paper ballots backup corrupted (or just malfunctioning) touch-screen or ballot marking devices.

- Practice recovery with professional staff, advisors and vendors by running drills and exercises. Theory is only theory. Practice makes it real.

Local election officials need support

It must be underscored – local election officials are the front-line troops in this battle. Those who control Federal, State, and local spending must provide local election officials with resources to do their job in this environment. Those who drive state election policies must make choices to fortify local officials for their new cyber mission.

Election officials are serving valiantly and professionally. They are talented and capable. They are holding the line. But they are operating with limited resources under sometimes unfair burdens placed upon them by policy makers in their respective states. Like good servants, they will say they can continue to hold the line. And they'll mean it.

But they need to be asked to hold a reasonable line. And holding a line that requires perfect defense every time is not reasonable.

It is impossible to defend against every conceivable attack. But if we detect breaches and recover from them quickly, we will survive any incident.

And so will faith in our democracy.