COOK COUNTY CLERK DAVID ORR
69 W. Washington, Suite 500, Chicago, Illinois 60602

TEL (312) 603-0996 FAX (312) 603-9788 WEB cookcountyclerk.com

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

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.

COOK COUNTY CLERK DAVID ORR
69 W. Washington, Suite 500, Chicago, Illinois 60602

TEL (312) 603-0996 FAX (312) 603-9788 WEB cookcountyclerk.com

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.