Grant Thornton

Public Sector

Five Ways to Mitigate Election Security Risks

The vulnerabilities uncovered in the 2016 election cycle were designed to undermine voter integrity and public trust. State and local government election officials are required to move beyond ensuring voting is free, fair and accessible, but also fostering the cybersecurity of our election processes.

Grant Thornton has defined the top five areas where government officials should initially focus limited resources to address risks to elections infrastructure and activities.

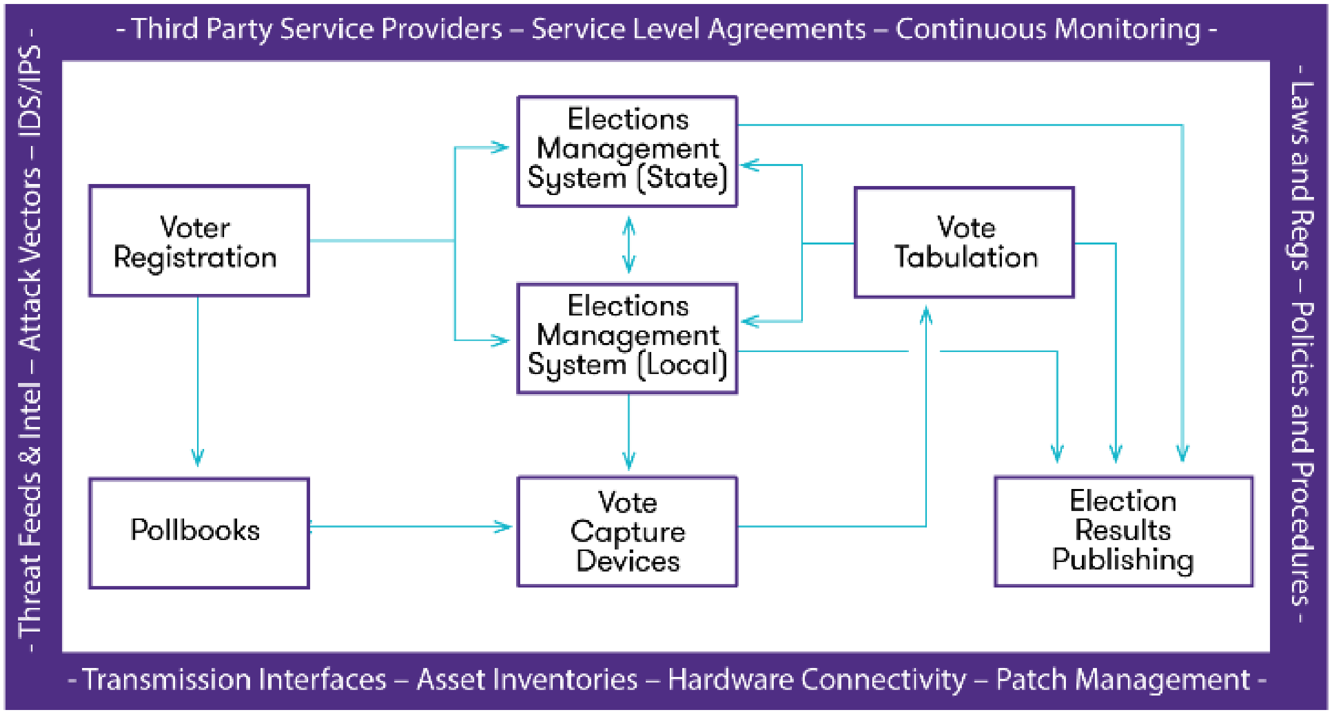
Grant Thornton's recommendations for improving elections infrastructure cybersecurity aligns with those found in the Center for Internet Security's (CIS) Handbook for Elections Infrastructure Security.

#1. Know what you're working with (Asset Management)

Understand all assets across your enterprise including the technologies being used, the interconnection of those technologies and the classifications of your data. This includes but is certainly not limited to vote capture devices and voting booth security. As important in your asset inventory are those systems that handle voter registration, pollbook creation, elections management systems, and results reporting – along with their underlying databases, interfaces and supporting infrastructure.

Where do I start?

- Enforce appropriate network segmentation;
- Conduct Discovery scans to validate architecture diagrams;
- Minimize footprint and interconnectivity of elections data;
- Establish a data classification process to classify and risk rank information and systems by confidentiality, availability, and integrity, but also by the level of connectivity (network connected, indirect connection, transmission, etc.).


- Third Party Service Providers – Service Level Agreements – Continuous Monitoring -
- Threat Feeds & Intel – Attack Vectors – IDS/IPS -
- Laws and Regs – Policies and Procedures -
- Transmission Interfaces – Asset Inventories – Hardware Connectivity – Patch Management -
Elections Management System (State)
Voter Registration
Vote Tabulation
Elections Management System (Local)
Pollbooks
Vote Capture Devices
Election Results Publishing

#2. Know your dance partners (Third Party Management)

IT infrastructure is increasingly dependent on third-party service providers for activities throughout the system lifecycle such as maintaining the infrastructure backbone, supplying hardware, security, and configuration management. Elections infrastructure is no different; however, the sensitive nature and focus of these systems increase the necessity to develop a thorough understanding of your supply chain, including all of your 3rd and even 4th parties.

Where do I start?

- Develop a comprehensive inventory of the end-to-end supply chain entities including up-to-date points of contact and how to reach them;
- Review applicable service level agreements (SLA's) and ensure they hold vendors accountable for security;
- Establish a common framework and minimum security standards to demonstrate;
- Periodically assess third-party risk and set up reporting metrics.

#3. Know your adversaries (Threat Intelligence)

Election security is not only about the integrity of the physical votes, but it is about restoring the American people's faith in the election process. Today's cyber environment demands we look outside of the typical threat intelligence feeds to gather information from non-traditional sources to understand the big picture. Disinformation promulgated in social media can be just as detrimental to your election security as a breach. Additionally, threat vectors like ransomware, denial of service attacks, phishing campaigns, and credential harvesting are getting significantly more sophisticated. Entities that integrate threat intelligence into their overall cyber program can pre-emptively prepare for, mitigate, or eliminate cyber incidents before they can make a substantial impact.

Where do I start?

Invest in tools and technology services to monitor and perform reconnaissance on social media, deep web, and dark web;

Join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC is sponsored by the U.S. Department of Homeland Security (DHS) and provides free awareness-related resources and services including:

- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Automated indicator sharing
- 24x7x365 Security Operations Center access
- EI-ISAC members-only discussion board
- Weekly elections security news alerts
- Elections sector quarterly report

#4. Plan, practice, plan again… (Incident Response)

The question election officials are facing today is not if a cyberattack will occur, but when. The difference between a front-page headline or a non-incident is having a robust response plan and process. Election offices can plan for a breach or incident and answer important questions like: how will you respond; how will you eradicate the breach; how will you communicate what has happened with the public. Once you have a response plan in place, you should test it by hosting a mock election and breach. The only way to know you can respond is to test your response.

Where do I start?

- Establish elections contingency plan;
- Integrate security breaches or technology outages into a “mock election” tabletop or functional exercise;
- Establish a communication plan for public, press, and other governmental agencies for if/when an incident occurs.

#5. Gain the Big Picture (Cyber Analytics)

Election official’s overseas assets across a geographically dispersed area, each with a different level of security skills. Once an organization understands all their assets they should use analytics to visualize the data and prioritize the risk response. Pulling all the disparate assets into a single dashboard allows you to monitor and mitigate the risk through a single view of your situation.

Where do I start?

- Select a common framework to assess against (NIST Cybersecurity Framework, Center for Internet Security (CIS) Elections Handbook, or a combination of both) to get an “apples-to-apples” view;
- Analyze and identify common vulnerabilities across the enterprise, but also use results to highlight where and how entities are doing things right;
- Use analytics to prioritize remediation efforts through integrating cost and timeline estimates.

CIS. Center for Internet Security®

Version 1.0 February 2018

A Handbook for

Elections Infrastructure Security

Contact Us

Dave Simprini
Principal
T +1 703 373 8698
E dave.simprini@us.gt.com

Rick Comeau
Senior Manager
T +1 518 915 6615
E rick.comeau@us.gt.com

GrantThornton

GT.com/publicsector

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the GTIL member firms provide audit, tax and advisory services to their clients, as the context requires. GTIL and each of its member firms are separate legal entities and are not a worldwide partnership. GTIL does not provide services to clients. Services are delivered by the member firms in their respective countries. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. In the United States, visit grantthornton.com for details.