Grant Thornton

Public Sector

Six ways to mitigate election security risks

The vulnerabilities uncovered during the 2016 elections were designed to undermine the integrity of the elections process and public trust.

State & local elections officials must now move beyond ensuring voting is free, fair and accessible, to also help ensure the cybersecurity of our elections systems and data.

With the 2020 Presidential Election fast-approaching, Grant Thornton has further strengthened its recommended areas where government officials should initially focus limited resources to address risks to elections infrastructure and activities.

Grant Thornton's updated, 6 recommendations for improving elections infrastructure cybersecurity align with those found in the Center for Internet Security's (CIS) Handbook for Elections Infrastructure Security. These suggested measures for reducing elections cybersecurity risk have also been validated and enhanced through lessons learned in the field at elections organizations.

#1. Know your elections systems

(Asset inventory management)

Understand all elections-supporting assets across your enterprise including the technologies being used, the interconnections of those technologies and the classifications of your data. This includes but is certainly not limited to vote capture devices (voting machines). Just as important in your elections asset inventory are those systems that handle voter registration, poll book creation, election management and vote tabulation, and election results reporting – including their underlying databases, interfaces and supporting infrastructure.

Where do I start?

- Conduct hardware & software discovery scans to validate systems architecture diagrams;
- Enforce appropriate network segmentation;
- Minimize footprint of elections data and interconnectivity of elections systems; and
- Establish a data classification process to classify and risk rank elections information and systems by confidentiality, integrity, and availability, as well as by the degree of network connectedness (fully network connected, indirectly connected, externally transmitted, etc.)

#2. Remediate your system weaknesses

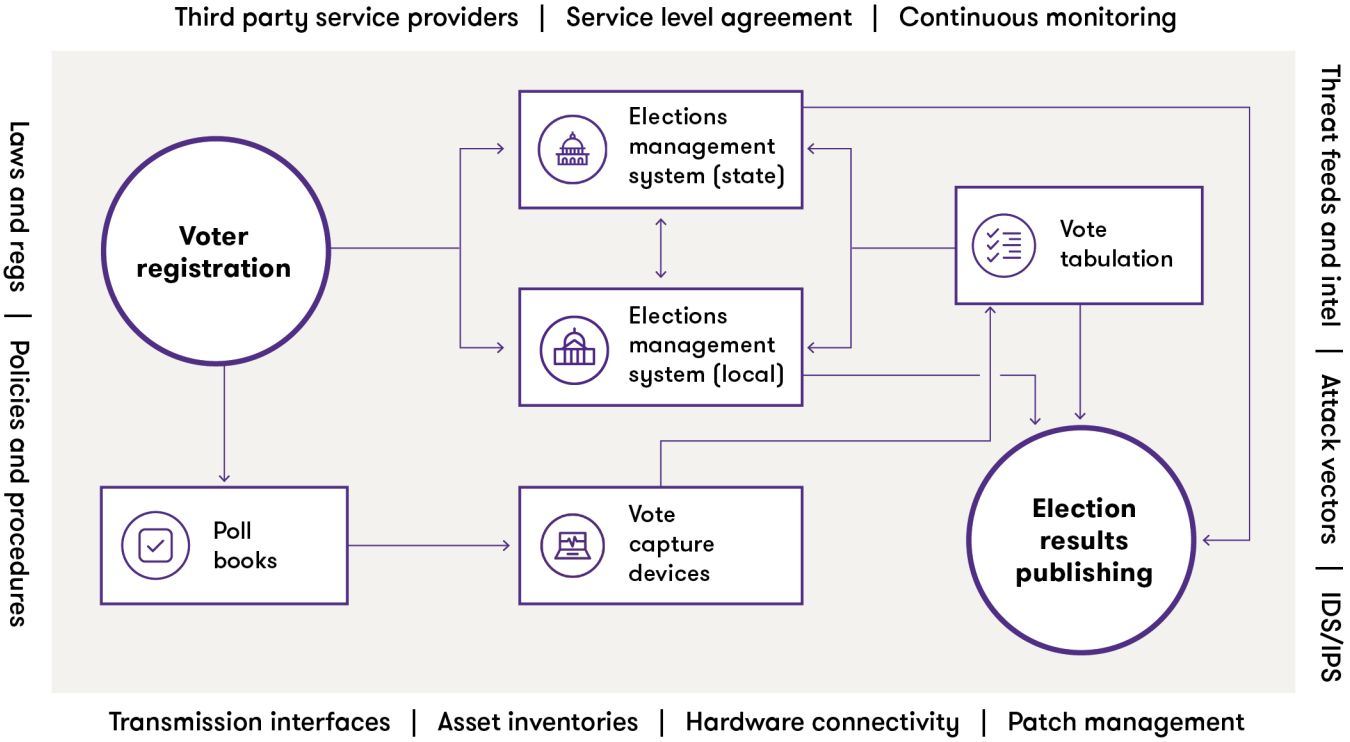
(Vulnerability & configuration management)

Like many state, and particularly local, government organizations, elections offices are severely resource constrained. Lack of necessary resources is especially problematic when it comes to constantly evolving information technology needs. Cybersecurity—both in terms of funding issues and a shortage of skilled technical experts—can be an even more daunting challenge for local governments and their boards of elections.

Software vulnerabilities are continuously identified in servers and desktop operating systems, database software, and applications that support both networked elections systems (e.g. voter registration databases) and those that are indirectly connected (e.g. election management systems, voting machines). Updating default, unsecure configurations and maintaining secure configuration baselines across an extensive, ever-changing inventory of IT systems and devices can also be extremely challenging.

Where do I start?

- Keep elections system hardware and software inventories up-to-date so you know what systems to keep updated on patching, etc.;
- Establish and implement a formal patch management program according to the security update schedules of relevant system & application vendors (e.g. Microsoft Patch Tuesday) and prioritize patch planning, testing, and application based on vulnerability severity and associated risk to IT assets;
- Establish and implement formal vulnerability and configuration management programs, ideally using a Security Content Automation Protocol (SCAP) scanner to identify and assess software and configuration-based vulnerabilities on a regular (at least quarterly) basis;
- Upgrade or replace end-of-life / obsolete systems and applications (e.g. server operating systems, database software), particularly those supporting the functionality of critical elections systems such as a voter registration database;
- Strongly consider uninstalling applications from elections-related servers and workstations where there is no business need for them, such as free music players, media players and .pdf viewers with frequent vulnerabilities, etc.; and
- Implement strong authentication (complex passwords at least 14 characters long) or, ideally, multi-factor authentication for all admin and user accounts on elections-related systems.



#3. Know your elections partners

(Third party management)

IT infrastructure is increasingly dependent on third party service providers for activities throughout the system lifecycle such as maintaining network and systems infrastructure, supplying hardware components and software updates, cybersecurity services, and configuration management. Elections infrastructure is no different. However, the sensitive nature and role of these systems increases the importance of developing a thorough understanding of your third party service providers, as well as clearly defining and agreeing to security responsibilities.

Where do I start?

- Maintain a comprehensive inventory your elections system and service providers, including up-to-date points of contact and how to reach them;
- Review applicable contracts / service level agreements (SLAs) and ensure they hold vendors accountable for the security of elections systems and/or services they provide, as well as for reporting any data breaches for which they may be responsible or aware;
- Establish a common framework-based, minimum set of security standards and requirements for demonstrating compliance; and
- Periodically assess third party risk and establish agreed upon reporting metrics.

#4. Know your adversaries

(Cyber threat intelligence)

Election security is not only about the integrity of physical votes, but about restoring the American people's faith in our democratic 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. Dis- information promulgated in social media can be just as detrimental to your elections security as a data breach.

Additionally, threat vectors like ransomware, denial of service attacks, phishing campaigns, and credential harvesting are becoming significantly more sophisticated. Entities that integrate threat intelligence into their overall cybersecurity program can pre-emptively prepare for, mitigate, and/or eliminate cyber incidents before they can cause substantial damage.

Where do I start?

- Invest in tools and technology services to monitor and perform reconnaissance on social media, deep web, and dark web; and
- 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 security awareness-related resources and services, including:
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Automated indicator sharing
- 24×7×365 Security Operations Center access
- EI-ISAC members-only discussion board
- Weekly elections security news alerts
- Elections Sector quarterly report

#5. Plan, practice, plan again…

(Incident response)

The question elections officials are facing today is not if a cyberattack will occur, but when. The difference between a front-page headline and a non-incident is having a robust incident response plan and process. Elections offices can plan for a data breach or incident and answer important questions like:

- How will you identify and respond to a suspected breach?
- How will you contain, eradicate, and recover from the breach?
- How will you communicate what has happened with the public, government partners, the media, etc.?

Once you have a response plan in place, you should test it by hosting a "mock election" including a cybersecurity incident scenario. The only way to know you can respond effectively is to test your response.

Where do I start?

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

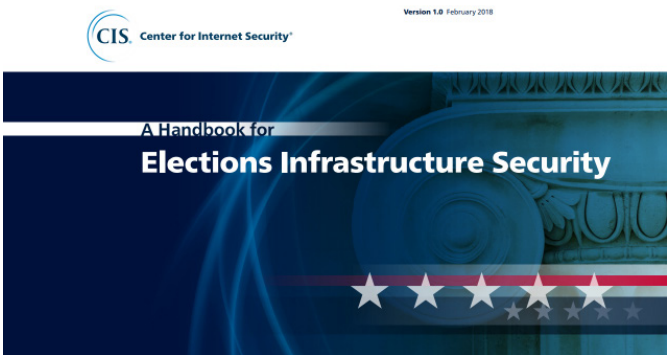
#6. Gain the big picture

(Cyber analytics)

Elections officials oversee numerous and complex assets across a geographically dispersed area, with elections jurisdictions each possessing a different level of cybersecurity proficiency. Once an organization identifies and understands all of its assets it should use analytics to visualize the data and prioritize associated risks. Pulling all of these disparate assets into a single dashboard allows you to monitor and mitigate the risk through a single view of your particular elections environment.

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 obtain an "apples-to-apples" view;
- Identify and analyze common vulnerabilities across the enterprise, but also use results to highlight where and how entities are doing things right; and
- Use analytics to prioritize remediation efforts through integrating risk severity / potential impact, prospective costs and timeline estimates.



Contacts

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

Grant Thornton

Grant Thornton Public Sector helps executives and managers at all levels of government maximize their performance and efficiency in the face of ever tightening budgets and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, and performance management. For more information, visit www.gt.com/publicsector.