WHITE PAPER

Defending the Castle:

PROTECTING YOUR ELECTIONS WITH DEFENSE IN DEPTH

HART intercivic™

Changes in the election security landscape require election officials to embrace a proactive mindset. Endeavors to improve practices and find and fix vulnerabilities are important to election security. This paper is written from the perspective of a voting system manufacturer that is continually focused on technology initiatives to protect the integrity of America's voting systems and critical infrastructure.

By applying defense in depth to each aspect of election preparedness—People, Processes, Procedures and Technology—you build a strong security framework with multiple, independent and redundant layers of protection and readiness.

Specific measures such as the air gap between the voting system and the Internet are essential to reliable protection. Still, no single tactic, however robust, can guard against every possible challenge to election security. This paper offers state and local election officials a sophisticated yet straightforward approach to fortifying security and protecting elections. Defense in depth is a deterrent to vulnerabilities in election preparedness and addresses the gamut of potential in both the technology side and the human side of modern democracy.[1]

SECURING THE MODERN-DAY CASTLE

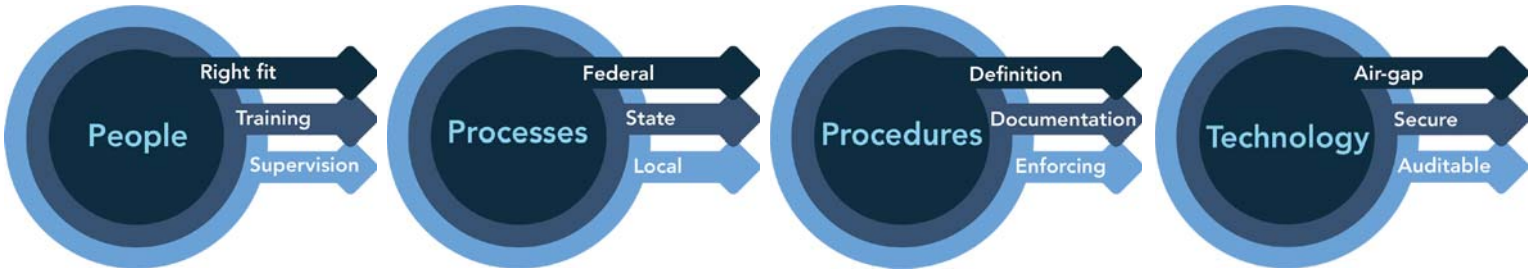
Back in medieval times, defense of a town and its resources was all about building the strongest castle. Then as now, castle design was both art and science. The mightiest castles had multiple layers of built-in defenses, from ditches and moats to thick, concentric layers of walls to specially designed ramparts for firing arrows down on attackers.

This layered approach is known as defense in depth, and it is an age-old approach to security encountered today, notably in the worlds of Internet and information technology. Like a castle, defense of a system starts at the perimeter firewall and is fortified layer by layer. It can be applied similarly to safeguard the world

1 U.S. Department of Homeland Security, 2016. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

of election security. Like the layers of protection of a castle, every aspect of election preparedness defends the integrity of the vote.

Modern, secure voting is effective when it is backed up by people who are focused on best practices and have the knowledge they need to do their jobs. In a nutshell, defense in depth is a way of thinking about the tasks you already do for each election. By applying defense in depth to each aspect of election preparedness—**People, Processes, Procedures and Technology**—you build a strong security framework with multiple, independent and redundant layers of protection and readiness.



People

Retired General Eugene Habiger, the former commander of U.S. strategic forces, has said, "Good security is 20 percent hardware and 80 percent culture." In other words, the human factor in election security is crucial. Fortunately, it is also the element most directly under your control. You can augment the capabilities of the people responsible for managing and defending elections by applying defense in depth thinking:

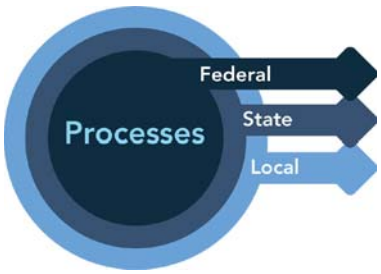
Right fit. Shield your elections with the right people with the right fit for the job. Perform background checks to confirm election officials and personnel as well as your temporary poll workers. Track changes in personnel with a tool such as a flow chart so that you know when someone moves into a position that requires a background check. Keep in mind to include not only staff who work directly in sensitive areas (for example, voter registration data) but also technical and systems staff.

Training. Protect against human errors or omissions by running comprehensive training for your personnel. Consider how and when the training is conducted as well as the content. What employees learn in training can be highly perishable, fading from memory after a few weeks. Time your training so that it is fresh for each election and reinforces the most important lessons. Cross-train staff so that you do not have one point of failure with respect to staff knowledge. Engage your voting system vendor to train personnel and provide step-by-step documentation.

Supervision. The innermost layer of defense of people is the supervision provided by you and your leadership team. Your staff naturally sees what is important to you and prioritizes commitments. Stay in the loop about security issues, and provide easy-to-read checklists that help poll workers. Make your involvement visible so that your elections personnel take election security as seriously as you do.

Processes

The election laws, code, rules and advisories adopted at the federal and state levels serve as the mortar fortifying the integrity of elections at the local level.



Federal. The U.S. Election Assistance Commission's VVSG (Voluntary Voting System Guidelines) is a strong basis for defining acceptable functionality, accessibility, accuracy, auditability and security capabilities for voting systems.[2] The Department of Homeland Security is developing a program that will also offer advice (and federal grants) to state and local jurisdictions to prepare for and defend against cyber incidents.[3]

State. Many states require testing of voting systems by independent third-party authorities before granting certification for sale within the state. State election laws, rules and advisories define the core processes that drive elections, including disciplined and structured security requirements.

2 U.S. Election Assistance Commission, 2018. Election Management Guidelines. *Chapter 1 Certification*. Retrieved from https://www.eac.gov/assets/1/6/Election_Management_Guidelines_-_Chapter_1_Certification.pdf

3 U.S. Election Assistance Commission, 2018. *Elections - Critical Infrastructure*. Retrieved from https://www.eac.gov/election-officials/elections-critical-infrastructure/

Local. What's not on your radar? Remember to examine the mundane aspects of safeguarding your elections. Even something as ordinary as the color of a pen can offer a level of defense. For instance, mandating that only red pens may be used in the room where ballots are adjudicated can thwart controversy involving ballots marked in blue or black ink. Do you know who has what data, when? Establish strong chain of custody processes that carry across all phases of election day to prevent manipulation of data during transfer from voting devices to a central count facility.

Procedures

While your election processes let you manage the big picture of how an election flows, your procedures define the nitty-gritty steps that each person follows to do their particular job.

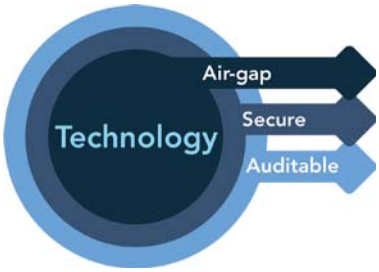
Definition. Outside of the processes that are defined at the federal and state level, each locality is entrusted to define the election procedures that work best.[4] The definitions you put in place can be your most valuable asset for training personnel, ensuring consistency and clearly spelling out roles and responsibilities. Where to start? Speak with peer election officials in other jurisdictions and seek out techniques that you can incorporate into your own procedures.

Documentation. Written documentation is vital to guarding defense in depth local procedures. Put procedures in place that heighten awareness of all elements that make up your world of election security. There is no room for informality in today's environment. Take the time to evaluate all procedures and create written documentation that supports your security goals. Then keep it up to date.

Enforcing. Do you know who has what data, when? Reinforce strong chain of custody processes across all phases of election day to prevent manipulation of data during transfer from voting devices to a central count facility. Remember: your procedures are your checklists. You already have them. Formalize your lists and keep them up to date. Cross-check procedures against state laws, rules and advisories; and share them with your peers for input.

4 U.S. Election Assistance Commission, 2017. *Election Workers Successful Practices.* Retrieved from https://www.eac.gov/documents/2017/08/01/election-workers-successful-practices-poll-workers/

Technology



No discussion of defense in depth is complete without a nod to the vital technical features and practices necessary for secure elections. Consider these aspects of a modern and secure system that incorporate defense in depth:

Air-gap. No part of a voting system should ever be accessible on the Internet or any other form of remote access. There should never be any direct connection with other systems such as voter registration data, electronic pollbooks or election night reporting systems.

Secure. All portals on your voting system that are not in use must be closed or otherwise disabled, with any attempt to tamper producing obvious physical evidence. Every digital device should be covered in your strong chain of custody protocol.

Auditable. Every system should have a log referencing who did what, and when. Logs are dependent on unique users, so make certain that you and your staff are not using generic logins to access your voting system. Follow your state rules for post-election audits, and invite the public to view your audit procedures and events.

In this changing environment, jurisdictions are best served by investing in a voting system that complies with these and other best practices and technical security protocols. Additional critical features include:

- Two-factor authentication
- Port obfuscation
- Whitelisting (only preapproved tasks can be executed)
- NIST/VVSG compliant encryption
- Authentication (hash codes) and digital signatures
- Kiosked workstations

Conclusion

Today's election officials cannot depend on any single measure to mitigate all security issues. Defense in depth is a timeless, practical strategy to secure voting systems and reduce risk. By applying a defense in depth approach to the four key areas of the security model—People, Processes, Procedures and Technology—election officials can deliver secure elections and foster confidence in the democratic process.

Your voting system vendor can be a valuable resource for information about how to protect elections in your jurisdiction. The following resources offer additional important reading:

"A Handbook for Elections Infrastructure Security," Center for Internet Security, https://www.cisecurity.org/elections-resources/

"Election Management Guidelines," U.S. Election Assistance Commission, https://www.eac.gov/election-officials/election-management-guidelines/

"Election Security Preparedness," U.S. Election Assistance Commission, https://www.eac.gov/election-officials/election-security-preparedness/

"System Certification Process," U.S. Election Assistance Commission, https://www.eac.gov/voting-equipment/system-certification-process-s/

"DHS Cybersecurity Services Catalog for Election Infrastructure," Department of Homeland Security, https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf

About Hart InterCivic

Austin-based Hart InterCivic is a full-service election solutions innovator, partnering with state and local governments to deliver secure, accurate and reliable elections. Working side-by-side with election professionals for more than 100 years, Hart is committed to helping advance democracy one election at a time. Hart's mission fuels its passionate customer focus and a continuous drive for technological innovation. The company's new Verity Voting system makes voting more straightforward, equitable and accessible—and makes managing elections more transparent, more efficient and easier. Only Hart offers a completely new, secure voting system that supports paper, electronic and hybrid voting.

15500 Wells Port Drive | Austin, TX 78728
www.hartintercivic.com | info@hartic.com | 800.223.HART