MANDIANT

MANDIANT CONSULTING
WHITE PAPER

A Phased Approach to Election Security and Checklist for Officials

As the next round of national and local elections draws closer, security experts expect nation-state threat actors, cyber criminals and malicious insiders will intensify their efforts to steal voter information, breach voting systems, conduct cyber espionage and influence activity to alter election outcomes.

Effectively blocking these threats can be a daunting challenge for government officials who must work with limited funds and manpower. Election officials need a holistic approach with world-class information, protection and threat response to stay ahead of threats. Mandiant recommends a phased approach to election security.

Each phase of an election requires specific areas of attention and resources must be allocated correspondingly to protect election infrastructure and preserve election integrity.

Phase 1: Prepare, harden and test to understand the environment

This phase takes place before an election, and its purpose is to proactively protect and harden security posture. It is intended to align cyber defenses across an organization's environment to best practices and current standards and support review. The threat environment must be properly defined in terms of potential adversary actions and motivations. In addition to evaluating the attack surface, cloud-connected assets and pollbooks, cyber experts should ensure previously undetected compromises have not occurred, harden external and internal vulnerabilities and validate control effectiveness. This phase is designed to achieve three outcomes for active cyber defense: baseline, visibility and validate.

Give election systems priority status

Like the power grid and water supplies, election infrastructure is an essential resource for local communities; the federal government now defines it as part of the nation's critical infrastructure. Government stakeholders must understand not only the associated cyber security threats but also the larger emergency management implications of breaches. For example, an attack on voting and registration systems may provide access to other essential services, such as networks used for public safety. Disruption to voting combined with the loss of essential services may result in political uncertainty, threats to public health and safety and even civil unrest.

Draw on expertise to create multiple layers of protection

Election officials should organize discussions with a broad range of stakeholders. This includes senior government executives, state homeland security directors, IT security personnel for the chief election officials, emergency managers, first responders, federal homeland security authorities and representatives from IT vendors. This collective experience helps ensure that an election security plan covers not only cyber threats but also addresses broader political, financial and social election concerns.

Extend security beyond internal operations

This includes the larger supply chain of public sector peers and private sector companies, such as cloud computing vendors that outsource portions of the IT infrastructure. Meet regularly with partners to review their security policies and identify any gaps that should be addressed in the run-up to elections. The federal government offers help for these reviews. The External Dependencies Management assessment offered by the United States Department of Homeland Security is a no-cost service for identifying and addressing technology risks associated with external partners.

Ensure that training is available, accessible and adequate

Elections rely on a voluntary workforce with diverse technical and operational skillsets. To ensure that processes and procedures are understood and followed throughout the election cycle, training must be available and appropriate for a minimal subset of the participants to understand and consume. Many election worker training programs are made readily available to volunteer staff members without consideration for access controls, sensitivity of content or overall integrity of the materials. Training can be used by threat actors to better understand the processes, procedures and attack surface being used and may help uncover gaps or paths for unauthorized access. Documents used for training should be protected with the same safeguards used for operational documents.

Implement proper vetting and screening process

Election staff comprises many volunteer local workers who are typically unvetted for their roles. With the rising risks of insider threats, the widening partisan divide and the need for election integrity, the election support workforce must be addressed not only from a criminal and personal safety perspective, but also from an ideological and mental health perspective to uphold the overall integrity of election results.

Phase 2: Test, monitor and defend to better anticipate threats

This phase is likely to include an increased risk of disruptive cyber attacks. Elevated active defense readiness postures are recommended. Priorities should include continuous validation of security controls and defense of critical assets. This phase focuses on better control over the access an adversary needs to achieve their goal. Threat hunting can help ensure an adversary does not maintain access to the organization's network and infrastructure. Do more enhanced hunting and monitoring for indicator-less behaviors. Assume attacks are happening and technical controls have missed something. Mandiant bases all actions in this phase on known and anticipated adversarial activities, using actual attacker malware, motivating factors, tactics, techniques and procedures. This phase provides three outcomes for active cyber defense: validation, integrity and decision advantage.

Test the plan

It's not enough to delineate responsibilities and policies for protecting systems and responding to threats as they unfold. Authorities must regularly test and continuously improve their election security plan. Run tabletop exercises with subgroups of stakeholders and with the full complement of people who are entrusted with election security to ensure everyone responds effectively under the pressure of an actual incident.

Modernize and test voting system infrastructure

Multilayered election security requires more than just an IT response; state and local governments must still shore up their digital defenses. Start by protecting pollbooks, voting tallies, voter records and related information as they pass through networks and reside in databases. Data generated with voting machines can be safeguarded by segmenting these machines on dedicated networks that aren't linked to external networks or the Internet. This reduces the chance that a cyber attacker can steal credentials or circumvent network defenses to access the data. Consider encryption technology to further protect information when it's in transit across networks, housed in databases or stored on hard drives or thumb drives. Enable and automate patching frequently to ensure software updates are applied as soon as they are made available.

Election infrastructure is used periodically throughout the year for the sole purpose of supporting elections. Systems are frequently set up, taken down, swapped in and out, maintained by a variety of personnel and non-personnel and replaced unexpectedly. While standards are recommended and maintained for critical systems they are generally not followed. Election infrastructure should be tested and validated for adequate and acceptable thresholds for patch management, change management, vulnerability eradication, configuration management and attack surface vulnerabilities.

Protect personal technology

Security experts warn that election officials may become bigger targets for attackers who try to tarnish the accuracy and fairness of elections. One tactic is to paint an official as being biased toward a candidate or party to bolster claims that election results were "rigged."

An appropriate defense is to make sure personal computing devices and home networks receive security similar to government agencies, with multifactor authentication, strong passwords, encryption and backup capabilities.

Phase 3: Respond, contain and remediate to withstand attacks

During an election, national, international and social media coverage often parallels real-time activity. Extensive intelligence on existing and emerging threat actor tactics, techniques and procedures enables effective and efficient incident response. Incident response services must have the capability to respond, contain and remediate critical security incidents with speed, scale and efficiency. This means using intelligence to establish resilience in a real-world threat environment.

Incident Preparedness

One of the best ways to know if you can respond to an incident is to test your preparedness. Mandiant Incident Response Preparedness Service helps you review your existing monitoring, logging and detection technologies so you can learn how you quickly contain an incident. Mandiant conducts a thorough review of current network and host architecture and evaluates your first response capabilities. Collaborative planning for typical response scenarios takes place to uncover recommendations for improvement.

Incident Retainer

The Mandiant Incident Response Retainer (IRR) allows you to establish terms and conditions for incident response services and lay the groundwork for immediate breach response or surge capabilities before a cyber security incident is suspected. With an Incident Response Retainer in place, Mandiant becomes your trusted partner on standby. This proactive approach can significantly reduce response time and the impact of a breach.

Post Incident Response

If an incident compromise does occur, the ability to restore core services and transform cyber defense is critical. Through ongoing services, customers can gain access to intelligence that provides accurate information regarding tactics, techniques and artifacts discovered and include threat hunting capabilities to assess the breach and related intelligence.

TABLE 1. Free Election Security Resources.

	Description
CISA	• No cost services • Access to regional cyber security personnel who can provide advice on preparing for and responding to cyberattacks • Cyber security assessments such as hygiene scans, risk and vulnerability assessments and cyber resilience reviews • Cyber threat hunting • Access to threat information, including the DHS Information Network portal; intrusion analysis after a cyber incident • Cyber security training and professional development opportunities • Election Infrastructure Security Resource Guide
CISA: FREE Cyber security Services and Tools	• CISA has compiled a list of free cyber security tools and services to help organizations further advance their security capabilities. This living repository includes cyber security services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cyber security community.
EI-ISAC	• Free cyber security services • Mis-/Dis-Information Sharing Service and Vulnerability Disclosure program
EAC	• Election security practices and toolkit • Quick start guides • Personal safety and incident response checklists • Anomaly reporting • HAVA funds • Glossary of commonly used cyber terminology
Department of Homeland Security	• Cyber security advisors and protective security advisors • Cyber security assessments • Detection and prevention • Information sharing and awareness • Incident response • Training and career development

TABLE 2. Election Security Checklist.

	Notes
Phase 1: Prepare, harden and test to understand the environment	
☐ Give election systems priority status • Understand associated cyber security threats and emergency management implications of breaches.	
☐ Draw on expertise to create multiple layers of protection • Organize discussions with broad range of stakeholders to address cyber threats and political, financial and social concerns.	
☐ Extend security beyond internal operations • Meet with partners to review security policies and identify gaps, evaluate the attack surface and cloud-connected assets, and perform pollbook security evaluations.	
☐ Ensure that training is available, accessible and adequate • Training must be appropriate and easily understood and documentation protected.	
☐ Implement proper vetting and screening process for election workforce • Election workforce selection must consider criminal, personal safety, ideological and mental health perspective.	
Phase 2: Test, monitor and defend to better anticipate threats	
☐ Test the plan • Run tabletop exercises, regularly test and continuously improve security plan	
☐ Modernize and test the voting system infrastructure • Consider encryption technology to protect election information as it moves through the network and test/validate infrastructure	
☐ Protect personal technology • Use multifactor authentication, strong passwords, encryption and backup capabilities on personal devices and home networks	
Phase 3: Respond, contain and remediate to withstand attacks	
☐ Incident preparedness • Test preparedness with collaborative planning for typical response scenarios	
☐ Incident retainer • Establish terms and conditions before an incident	
☐ Post incident response • Plan for ongoing services with access to threat intelligence and threat hunting capabilities	

Additional Resources:

- Mandiant (2022). A Tiered Framework for Cyber Threat Levels.
- Mandiant (2022). The Defender's Advantage Cyber Snapshot. Protecting Societal Events When the Whole World is Watching
- Mandiant (2022). Proactive Preparation and Hardening to Prevent Against Destructive Attacks.

Learn more at **https://www.mandiant.com/solutions/defending-elections-against-cyber-threats**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE