



MITIGATING INSIDER THREATS TO U.S. ELECTION SYSTEMS

OVERVIEW

Elections in the United States are administered at the state and local levels of government, creating a diverse landscape of election systems and technologies across the country. Our national exercise in self-government also requires the support of vast groups of people, including election workers, vendors, contractors, temporary workers, and volunteers. Ensuring that our elections remain secure and free from interference requires thoughtful screening practices to manage the risks associated with providing access to sensitive systems.

The Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Election Assistance Commission (EAC) prepared this overview to help partners mitigate the risk posed by potential insider threats during the 2026 election cycle.

Practices that deter, detect, or prevent harm caused by insiders are an integral part of conducting secure elections. This guidance assists those working in election infrastructure to establish or improve insider threat mitigation programs.¹

What is an Insider Threat?

An [insider threat](#) describes the potential for an insider to use their authorized access, intentionally or unintentionally, to do harm to an organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the security of the organization, its data, personnel, or facilities. Insider threats also include the risk that an individual's access or knowledge of systems could be exploited by foreign adversaries, criminal networks, or other malicious actors.

Unintentional Threats

The majority of insider threats are unintentional, either through negligence or accident. For example, an individual might be aware of but ignore security or information technology (IT) policies, creating risk to the organization. These behaviors can often be corrected.

Collusion

Insider threats may arise from recruitment by external threat actors for compromise, disruption, fraud, or espionage. Such threats are often surreptitious and therefore difficult to detect.

Intentional Threats

Insiders might intentionally harm an organization for personal benefit or to act on personal grievance. Others may have a desire for recognition and seek attention by creating danger or divulging sensitive information. They may even think they are acting in the public good.

Third-Party Threats

Third-party threats arise from individuals from outside of an organization that have been granted access to facilities, systems, networks, or people and can also be intentional or unintentional.

¹ The FBI and CISA encourage the public to report information concerning suspicious or criminal activity to their local FBI field office (www.fbi.gov/contact-us/field).

Election-Related Insider Threats

In most jurisdictions, election officials administer elections with assistance from temporary or seasonal staff, volunteers, vendors, and contractors. Given that any person with privileged access may pose an intentional or unintentional insider threat, local election officials are encouraged to follow established best practices and clearly identify the level of access afforded to different personnel.

Vendors and Contractors should be held to the same security standards as employees. Officials should consider restricting or eliminating remote access to election systems or assets by contractors, limiting access to only systems and data required to perform the contracted service, and having the appropriate government officials present when contractors access critical systems or data (but at minimum, always require that at least two people are present). When possible, set up separate vendor and contractor accounts from those of regular employees and utilize devices managed by the election office to prohibit untrusted devices on the network. Consider providing individuals with identifiable badges when they are working at government facilities so it is easy to identify who should or should not be in secure areas.

Temporary Staff, Seasonal Staff, and Volunteers recruited to support the conduct of elections should understand the mission of the election office and possess a high degree of accountability for their role. Upon joining the team, all new members should be required to sign a code of conduct that clearly outlines expected behavior and describes consequences for violations. Temporary staff and volunteers should be retrained on systems, data, and security practices prior to every election. Standard operating procedures (SOPs) and chain of custody procedures should include guidance for all role types, including temporary staff and volunteers. This may include use of the two-person rule, or control forms, which can be effective measures for temporary staff and volunteers to check each other's work, deter harmful behavior, and verify compliance.

Examples of Unintentional Threats to Elections:

- Allowing someone to “piggyback” through an access-controlled ballot tabulation room door
- Misplacing or losing portable storage devices or media containing sensitive voting system data
- Ignoring messages to install new software updates or security patches
- Mistyping an email address and accidentally sending a sensitive document externally
- Unknowingly or inadvertently clicking on a hyperlink in a phishing email
- Improperly disposing of sensitive voter data

Examples of Intentional Threats to Elections:

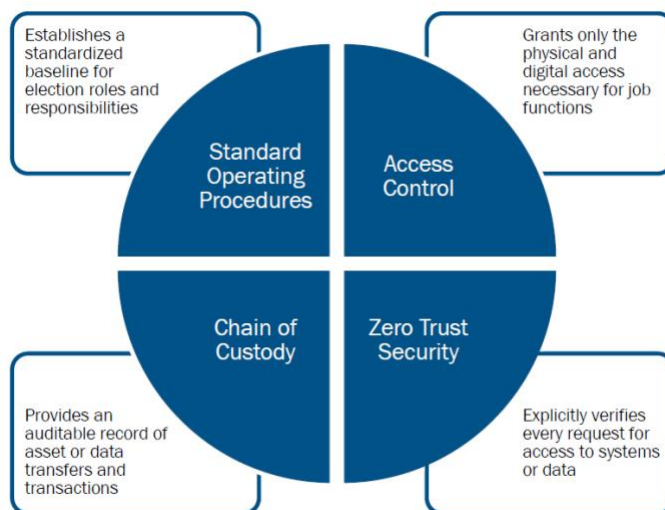
- Altering or attempting to alter or destroy ballots, mail-in ballot envelopes, registration forms, or other core election documents
- Accessing systems, equipment and/or facilities without need or authorization with the intent to misuse, delete, or corrupt data
- Turning off security cameras or access control systems or disregarding two-person rule requirements to allow unauthorized access to controlled areas or controlled information
- Disregarding information systems policies related to installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information with the intent to disrupt systems, or corrupt or steal sensitive data

Securing Your Organization: Building an Insider Threat Mitigation Program

Most longstanding election practices are designed to ensure the integrity of the voting process, from handling ballots in teams of two (often bipartisan), to robust chain-of-custody procedures, to the presence of observers during voting and ballot counting. Nevertheless, election infrastructure stakeholders may benefit from documenting their approach and establishing a formalized insider threat mitigation program. These actions can help identify gaps in current practices and inform the organization's broader approach to risk management.

Organizational culture should reinforce proactive reporting of employee concerns and security issues as a core component of securing the environment. From this foundation, a successful insider threat mitigation program should implement practices, strategies, and systems that limit and track access across organizational functions. Provided they receive the necessary oversight to ensure they are being applied appropriately, preventative measures against insider threats also contribute to detecting threats by establishing transparent, auditable election systems and processes and then identifying outliers or anomalies for investigation.

Key elements of election infrastructure insider threat mitigation programs include:



Standard Operating Procedures (SOPs) describe the sequence of steps or requirements to complete a task. Examples can include requiring visual signs to identify authorized personnel in specific areas, requiring a “buddy system,” or a two-person minimum for handling of sensitive tasks. Logs and checklists are helpful tools for promoting adherence to SOPs. Include processes in election technology contracts with vendors and manufacturers to ensure compliance with the required security measures.

Physical and Digital Access Control should apply the principle of least-privilege, giving individuals access only to systems required to perform their essential functions. Access privileges may change leading up to an election or other key dates. Physical access controls may include limiting access to facilities, equipment, devices, tamper-evident seals and bags, and other assets as well as providing video surveillance of physical assets. Digital access controls grant access only to necessary systems, assets, data, or applications related to an individual’s job or function.

In both cases, access logs, control forms, and surveillance video provide auditable records of who accessed a physical or digital asset and when it was accessed. Overall, access control systems prevent any one individual from gaining entry to all assets within an organization and reduce potential harm to physical or digital systems. If an incident is suspected, access logs and control forms can help with post-incident investigations and even serve as evidence.

Chain of Custody Procedures track the movement and control of physical and digital assets by documenting each time an asset is handled or transferred and who was responsible. This can help prevent unauthorized access to sensitive systems, detect the presence of an insider threat, provide evidence, and shorten remediation time if an incident occurs. It produces an auditable record of asset transfers and transactions, enabling detection of a potential threat if there is a gap in the chain of custody.

Zero Trust Security is based on the principle of “always verify.” Instead of assuming everything that happens on an organization’s networks and systems is safe, the zero-trust approach assumes a breach has or will occur and verifies each request as though it is unauthorized. A zero-trust approach explicitly verifies every request for access, regardless of where it originates or what resource it accesses. Many digital systems now include zero trust security features that can be turned on, such as always requiring users to enter their password rather than storing it in the device’s memory. Election officials may also consider procedures like implementing the “two-person rule” (require at least one observer to be present) or working in bipartisan teams when accessing sensitive resources.

Additional Mitigation Techniques Can Include:

- **Conduct risk assessments** to identify an organization's risks and provide early warning of potential insider threats.
- **Provide training** to reduce the risk of unintentional harm, clarify policy, improve response time, and support compliance and audit requirements.
- **Monitor for anomalous behavior** with a combination of human and digital tools—such as access logs, video surveillance, endpoint detection and response software—underpinned by a strong organizational culture of proactive reporting.
- **Audit all election and business processes** before, during, and after an election. Audits validate whether measures such as access control and chain of custody are functioning properly, whether necessary data is being collected and maintained, and whether it is being used appropriately by staff. They also provide the opportunity to review records (access logs, security footage, chain of custody forms, etc.) and identify any potential gaps or areas for improvement.
- **Follow cybersecurity best practices** to reduce the risk of a system compromise. Cybersecurity best practices like multi-factor authentication, patching and updating, and network segmentation all help minimize the potential security impact if an incident, like an insider threat, were to occur.
- **Report all incidents** to the appropriate authorities so they can be investigated, documented, and reduce the likelihood of similar incidents occurring in the future.

Measures such as establishing and maintaining necessary standard operating procedures, access controls, zero trust security, and chain of custody procedures are necessary facets of election administration. Further, they must be reviewed, tested, and audited before, during, and after elections. Altogether, these measures support the integrity, reliability, and security of an election, providing evidence to build public confidence in the process.

Assessing Insider Threats

Insider threat assessment is the process of compiling and analyzing information about a person of concern who may have the interest, motive, intention, and capability of causing harm to an organization or persons, with the goal of preventing a security incident. Because individuals demonstrate unique baseline behavior, what is suspicious behavior in one person may not be suspicious behavior in another. When analyzing potential insider threat behaviors, it is important to keep in mind the whole person approach which assesses whether or not behavior is abnormal based on an individual's standard baseline of behavior and habits. The appropriate workplace authorities conducting the investigation should answer several key questions:

1. Is there evidence to suggest the person of concern poses a threat?
2. What type of threat does the person of concern pose?
3. Is the person of concern moving towards committing a malicious act?

Non-Emergency Intervention

If there is no immediate threat, then the organization should begin, to the extent authorized by law, a deeper investigation to gather information, evaluate the risk, and determine next steps. The purpose of the investigation is to gather evidence (including access control systems, security logs, and chain of custody forms), determine the person of concern's baseline behavior and changes from it, analyze the risk of moving towards a malicious act, and document the findings. Based on the investigation, the team can determine next steps, which may include, but are not limited to, watching and waiting, changing or restricting access privileges, taking administrative action such as suspension or termination, and/or assisting with finding outside counseling or support, and/or reporting to law enforcement.

Emergency Intervention

If emergency intervention is required based on the initial screening, the organization should take immediate action, including calling for assistance from first responders or law enforcement if necessary. Organizations should coordinate with local law enforcement to conduct walkthroughs and site visits, and familiarize first responders with the organization or facility emergency action plan before any potential incident requiring their response.

Managing Insider Threats

Effective insider threat mitigation requires that organizations foster a positive, supportive culture that prioritizes security best practices. Integral to this goal is a transparent and consistent process for reporting, investigating, and assessing unusual behavior, where both staff and the public know that their reports will be acknowledged, taken seriously, and handled appropriately. Programs that encourage early reporting and intervention increase the likelihood that a threat, whether intentional or unintentional, can be mitigated or deescalated. Once an issue has been resolved or mitigated, consider organizing a debrief session for appropriate stakeholders to discuss the issue, the steps that were taken to mitigate it, and areas for improvement.

[CISA's Insider Threat Mitigation webpage](#) includes more information, guides, templates, and other resources that can help election officials review and incorporate best practices into their insider threat mitigation efforts.

Additional Election Security Resources and Contacts

Suspicious or criminal activity can be reported to local FBI field offices. Their contact information is available at: fbi.gov/contact-us/field.

For additional assistance and best practices, please visit the following websites:

- [Election Crimes and Security | FBI](#)
- [Election Security | CISA](#)
- [Election Security | U.S. Election Assistance Commission \(eac.gov\)](#)
- [Election Security | Homeland Security](#)
- [Insider Threat Mitigation Guide | CISA](#)