Election Infrastructure Insider Threat Mitigation Guide

INTRODUCTION

Individuals entrusted with access to election infrastructure can, at times, represent potential risks to the confidentiality, integrity, and availability of election systems and information. This includes current and former employees, volunteers, contractors, and any other individual who has been granted privileged access to election systems and information. Across all critical infrastructure sectors and in virtually every organizational setting, trusted insiders have the potential to cause intentional or unintentional harm.

Practices that deter, detect, or prevent harm caused by insiders are an integral part of conducting secure elections. This guidance assists those working in the election infrastructure subsector to improve existing insider threat mitigation practices and establish an insider threat mitigation program, and summarizes and expands upon select guidance from previously issued CISA resources on insider threat mitigation for critical infrastructure stakeholders.

DEFINING INSIDER THREATS[1]

Insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

Unintentional Threats

Insider threats can be unintentional, including cases of negligence or accidents.

- **Negligent**: Insiders can expose an organization to harm by their carelessness. Insiders of this type are generally familiar with security and/or IT policies but choose to ignore them, creating a risk to the organization. Negligent insiders are usually complacent or show an intentional disregard for the rules. They exhibit behaviors which can be witnessed and corrected.
- **Accidentals**: Even the best employee can make a mistake causing an unintended risk to the organization. Organizations can implement strategies to limit risk, but accidents may still occur. While accidents can't be fully prevented, risk can be reduced through training and appropriate controls.

Intentional Threats

Insiders can intentionally take actions that harm an organization for personal benefit or to act on a personal grievance. Some intentional insiders are motivated by a disgruntlement related to a perceived grievance, ambition, or financial pressures. 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.

Other Threats

In addition to insider threats involving only insiders at an organization, insider threats may also involve individuals external to the organization. These collusive and third-party threats may be either unintentional or intentional.

- **Collusion**: This threat occurs when one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, sabotage, or a combination of these. This type of insider threat can be challenging to detect, as the external actors are typically well-versed in security practices and strategies for avoiding detection.
- **Third-Party Threats**: Third-party threats are associated with contractors or vendors who are not formal members of an organization, but who have been granted access to facilities, systems, networks, or people to complete

[1] Definitions sourced from: "Insider Threat Mitigation Guide." Cybersecurity and Infrastructure Security Agency, 2020. https://www.cisa.gov/sites/default/files/publications/Insider Threat Mitigation Guide_Final_508.pdf

their work. This type of threat can involve collusion among multiple third-party entities. Third-party threats may be direct, where specific individuals compromise a targeted organization, or indirect, where there may be flaws or outdated systems exposing the organization to unintentional or malicious threat actors.

Examples of Unintentional Threats

- Allowing someone to "piggyback" through a secure entry point
- Misplacing or losing portable storage devices or media containing sensitive information
- Ignoring messages to install new software updates or security patches
- Mistyping an email address and accidentally sending a sensitive business document externally
- Unknowingly or inadvertently clicking on a hyperlink or phishing email
- Improperly disposing of sensitive documents or data

Examples of Intentional Threats

- Attempting to alter or destroy ballots, mail-in ballot envelopes, registration forms, or other core election documents
- Attempting to violate ballot secrecy
- Attempting to alter or destroy elections data, including voter registration data
- Allowing an unauthorized person to access election equipment, systems, assets, or data
- Turning off security cameras or access control systems
- Stealing election equipment or data
- Leaking confidential information to the press or public
- Intimidating or threatening other staff

Expressions of Insider Threat

Insider threats manifest in various ways, including violence, espionage, sabotage, theft, and cybersecurity incidents.

- **Cybersecurity Incidents**: These include a range of actions, which may include theft, espionage, violence, or sabotage, dealing with anything related to technology, virtual reality, computers, devices, or the internet. These actions are undertaken using a variety of vectors such as viruses, data breaches, denial of service attacks, malware, or unpatched software, and can be either unintentional or intentional.
- **Violence**: An act of violence, threats of violence, or other threatening behavior that creates an intimidating, hostile, or abusive environment. Insider violence includes criminal or destructive threats, which precede a physical attack, and damage infrastructure or harm the health and safety of an individual or organization. This can include terrorism or workplace/organizational violence.
- **Espionage**: The practice of spying on a foreign government, organization, entity, or person to covertly or illicitly obtain confidential or sensitive information for military, political, strategic, or financial gain. This includes criminal, economic, or government espionage.
- **Sabotage**: Involves deliberate actions aimed at harming an organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or modifying or deleting code to disrupt operations.
- **Theft**: Theft involves multiple types of stealing, most often involving finance or intellectual property. Financial crime is the unauthorized taking or illicit use of a person's, business', or organization's money or property with the intent to benefit from it. Theft also includes intellectual property theft, or the robbery of an individual's or organization's ideas, inventions, and/or creative expressions. Digital systems containing large quantities of customer data or intellectual property may be more appealing to bad actors.

WHAT IS MDM?

CISA uses the following definitions for mis-, dis-, and malinformation (MDM). MDM can originate from both foreign and domestic sources.

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Insider Threats and Mis-, Dis-, and Malinformation

The information environment surrounding elections, and particularly the spread of election-related mis-, dis-, and malinformation (MDM), may provide additional motivation for insider threats. MDM content is often designed to elicit a strong emotional response from the consumer and bypass logical reasoning to incite action, whether the action is simply spreading the content further on social media or taking action in the real world, including acts or threats of violence. A common tactic deployed by both foreign and domestic MDM actors is to reinforce a strong sense of belonging, community, and in-group mentality among those who regularly consume their content. In instances where an individual already has a grievance with an organization or is experiencing other stressors in their life, MDM narratives may provide an alternate interpretation of reality that appears preferable to real life. This vulnerability can lead to or exacerbate insider threats.

While election infrastructure stakeholders cannot predict or fully control the information environment around elections, they can educate their staff, volunteers, and vendors about MDM narratives and tactics. Ongoing training and education opportunities are especially important for non-full-time staff, who may not join the organization with full knowledge of election processes or how they may be impacted by MDM content. Similarly, election infrastructure stakeholders can mitigate the impact of MDM narratives through proactive and consistent communication with the public about election processes. Such communication can help avoid fueling MDM narratives and build organizational resilience against them. When communicating about election processes, election infrastructure stakeholders should aim to provide straightforward, concise information without being overly detailed or causing more confusion.

The current MDM environment, at the local, national, and international level, should be considered when assessing insider threats. Transparent communication, in conjunction with the prevention and detection measures described below, can help staff understand and perform their role, connect it to the organization's mission to administer secure elections, and stay resilient against potential MDM narratives that undermine that mission and potentially incite insiders to cause intentional harm.

BUILDING AN INSIDER THREAT MITIGATION PROGRAM

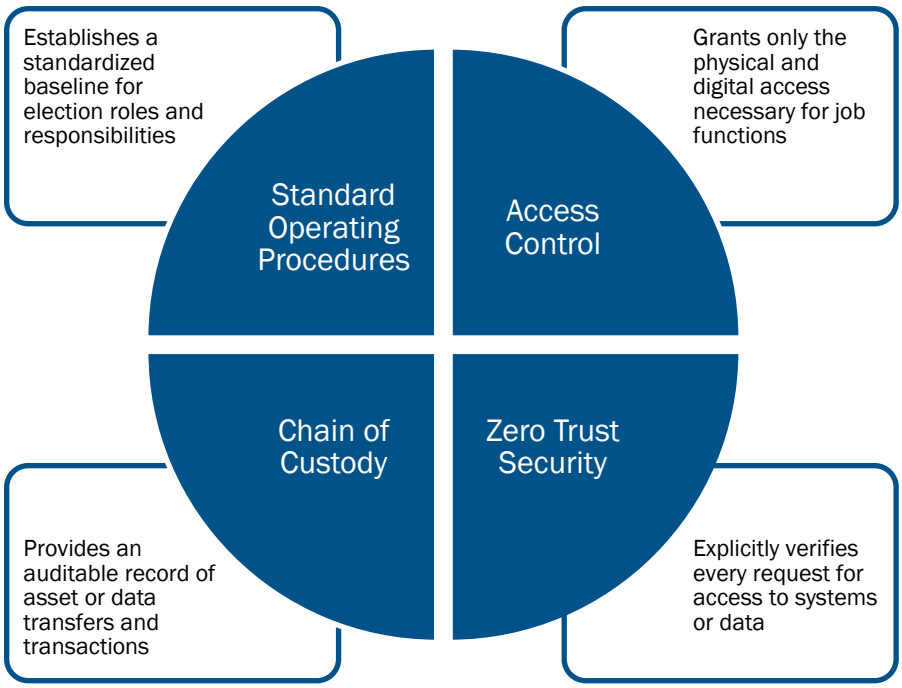
Election officials and their private sector partners regularly employ practices designed to deter, detect, or prevent harmful acts by insiders -- whether or not they use the term "insider threat" or have articulated their approach and practices in a documented program. From handling ballots in teams of two, to robust chain-of-custody procedures, to the presence of observers during voting and counting, many longstanding core election practices have been designed with insider threat mitigation in mind. Nevertheless, election infrastructure stakeholders may benefit from documenting their approach and establishing a more formalized insider threat mitigation program. Such actions can help identify gaps in current practices and inform the organization's broader approach to risk management.

Successful insider threat mitigation programs employ proven practices, strategies, and systems that limit and track access across organizational functions, services, and applications. Those practices and systems limit the amount of damage an insider can do, whether the act is intentional or unintentional. A holistic, multi-layered approach to insider threat mitigation combines physical and digital security with personnel engagement. An effective mitigation program aims to understand the insider's interaction within an organization, track the interaction as appropriate and permitted by law, and intervene if the interaction poses a threat to the organization. An organization's insider threat mitigation program is an essential component of the broader organizational risk management plan.

A strong foundation for insider threat prevention and mitigation comes from a set of values that are shared and acted upon by everyone in the organization. **Organizations should promote a positive climate of accountability, transparency, and trust.** Organizational culture should also reinforce employee reporting as a core component of securing the environment.

Key Elements of Election Infrastructure Insider Threat Mitigation Programs

From a foundation of a proactive and supportive culture, election infrastructure stakeholders can implement several proactive and preventive measures to reduce the risk and impact of insider threat activity. While each aspect is individually important, they are most effective when implemented together to create a comprehensive, resilient election administration environment. Key elements of election infrastructure insider threat mitigation programs include: establishing robust standard operating procedures (SOPs), managing physical and digital access control, deploying zero trust security principles, and implementing chain of custody processes.



Standard Operating Procedures

Establishing and implementing SOPs primarily helps prevent unintentional insider threats due to negligence or accidents. SOPs outline how organizational functions should be performed and standardize the various tasks and responsibilities associated with different roles, increasing the quality and consistency of work across staff. Especially in an election environment, where volunteers and third-party vendors turnover regularly, SOPs can help employees onboard quickly, understand the expectations of their role, and successfully perform their duties. Further, SOPs create a baseline against which to measure outcomes and identify areas for increased efficiency and improvement.

SOPs for each role or responsibility should clearly document the steps needed to perform the activity successfully. This includes providing sequential steps for task completion, showing visuals and examples, and specifying the checklists and logs necessary for verification. Incomplete or nonexistent SOPs may cause staff to develop their own procedures, which may induce additional risk. SOPs therefore limit *ad hoc* decision making and can help speed the remediation process should issues arise.

Access Control

Physical and digital access control systems both prevent and detect insider threats. 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, as well as when it was accessed. Overall, access control systems prevent any one individual from gaining entry to all assets within an organization, reducing potential harm to physical or digital systems. If an incident is suspected, access logs and controls forms can help identify who is responsible for potentially harmful behavior.

Access control systems should apply the **principle of least privileged access** to grant all individuals (full-time staff, volunteers, and vendors) access only to systems and data required to perform their essential functions. Access privileges may change leading up to an election or other key dates. Additionally, organizations should ensure that access is promptly revoked when an individual concludes their work or leaves the organization (e.g., turning off facility access for vendors once they complete routine maintenance).

A key challenge around access control for election officials is access to the state voter registration database system. The state may not know who has access within each local election office, so it is important for jurisdictions and state offices to work together to regularly confirm and update a list of authorized users and associated privileges.

Zero Trust Security Principles

A zero trust approach to security is based on the principle of "always verify." Instead of assuming that everything that happens on an organization's networks and systems is safe, the zero trust approach assumes that a breach has or will occur and verifies each request as though it is unauthorized. Previously, in many organizations, the security of digital assets was closely tied to the physical location where they were stored and universal trust in all members of the organization. In other words, all devices in an office and all staff users could access most information, systems, and data. This implicit trust of devices or users made it easy for insider threats to manifest in an organization undetected. In contrast, the 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 infrastructure stakeholders 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.

Visit https://zerotrust.cyber.gov/ for additional guidance on zero trust implementation from CISA and the Office of Management and Budget (OMB).

Chain of Custody

Chain of custody is a transparent process to track the movement and control of physical and digital assets by documenting each person and organization that handled an asset, sensitive equipment, or data; the date and time it was collected, transported, or transferred; and why the asset was handled. While not unique to elections, chain of custody plays a vital role in ensuring the integrity of an election and providing evidence in the event an insider threat is detected, as well as improving remediation time if an incident occurs. Without robust chain of custody practices, election systems equipment, assets, or data at rest or in transit could be unknowingly accessed and manipulated by threat actors.

Elections are complex, and there are many functions that make up the intricate process of conducting an election. At every point where data, media, or equipment are entered, accessed, transferred, transmitted, or stored, there is an opportunity for error or risk. Robust chain of custody practices reduce this risk by creating an auditable trail of assets throughout the election process.

To address risk and improve security and resilience, election infrastructure stakeholders can utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to establish chain of custody standards, guidelines, and practices. NIST outlines a five-step process to identify assets and risks, protect systems, detect incidents, respond to breaches, and recover.

Example: a chain of custody procedure could require that at least two people sign all equipment, transported materials, or media access logs: the primary user and a witness who ensures the equipment, , media, or other assets were appropriately handled. Absent this requirement, it may be difficult to verify who accessed or transported the equipment, media, or other assets and for what purpose.

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 the evidence to build public confidence in the process.

ELECTION INSIDER THREATS IN FOCUS

In most jurisdictions, election officials administer elections with assistance from temporary or seasonal staff, volunteers, vendors, and contractors. Similar to potential threats posed by full-time staff, such individuals may pose an insider threat. Therefore, election officials should ensure that all individuals involved in elections are considered, based on their specific roles and responsibilities, when developing an insider threat mitigation program.

Vendors and Contractors

Vendors and contractors should be held to the same level of security standards as employees. Election officials should ensure that they build into their procurement processes and contracting requirements the same safeguards that they hold their own employees to. When acquiring new contracted services, security requirements and minimum qualifications should be built into requests for proposals and in the final contractual agreements, such as mandatory background checks for all individuals who will be working on the contract.

Vendors and contractors will likely have the same or greater physical and/or digital access to certain critical data that full-time staff do, and they therefore bring similar, if not increased, risk to election infrastructure. Election 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 when possible, having a government official present when contractors access critical systems or data (but at minimum always require that at least two people are present). When possible, segregate vendor and contractor accounts from those of regular employees and utilize devices managed by the organization to prohibit untrusted devices on the network. Consider providing individuals with a colored lanyard, badge, vest, or similar item when they are working at government facilities so it is easy for all to identify who should or should not be in secure areas.

Temporary Staff, Seasonal Staff, and Volunteers

Most election offices rely on temporary, seasonal, and/or volunteer workers to conduct polling operations, including the operation of election equipment and transporting sensitive media or election materials, process voter registration forms, handle mail-in ballot request forms, manage mail-in ballots, and other election administration tasks. Building a successful team of temporary and volunteer staff starts with the recruitment of individuals who understand the mission of the organization and possess a high degree of accountability for their role. Upon joining the organization, all new members should be required to sign a code of conduct that clearly articulates expected behavior and outlines consequences for violations.

In addition to the considerations above, temporary staff and volunteers should be retrained on systems, data, and security practices prior to every election. It is especially important to provide updated training on MDM trends, including MDM risks specific to the state or jurisdiction. Finally, 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 an effective measure for temporary staff and volunteers to check each other's work, deter harmful behavior, and verify compliance.

DETECTING AND IDENTIFYING INSIDER THREATS

Even the most robust preventive and protective measures cannot fully eliminate the risk of intentional or unintentional insider threats. Therefore, it is important for election infrastructure stakeholders to routinely test and audit their procedures, which will aid in identifying procedural gaps and responding to evolving threats in elections. Threat detection takes place through both human review and technical tools that monitor for the presence of threat indicators.

As those who perpetrate violence or steal data often share their plans or grievances with others before acting, coworkers, peers, friends, neighbors, family members, or casual observers are frequently positioned to have insight into and awareness of predispositions, stressors, and behaviors of insiders who are considering malicious acts.

Each individual has a baseline of behaviors and straying from their norm could be an indication that something about them has fundamentally changed. Important to the process of identifying potential threat indicators is understanding that **behavior is what matters most**, not the motivation. The presence of political, religious, ideological, financial, or revenge-based motivations helps to understand what drives an individual to act, but the individual's behavioral indicators are the key to determining whether they warrant additional consideration, monitoring, or assessment as a potential threat.

Insider Threat Preventative Measures as Detection Mechanisms

Preventive measures against insider threats, including SOPs, access control systems, zero trust security, and chain of custody, also contribute to detecting and identifying threats by establishing transparent, auditable election systems and processes. However, effective detection via these measures requires human understanding and oversight to ensure they are being applied appropriately and audited routinely to identify outliers for further investigation. Having preventive measures in place means little if they are not consistently used.

Each measure can aid threat detection in the following ways:

- **Standard Operating Procedures**: SOPs and best practices provide a common baseline for a team to measure against and detect when best practices are not being followed.
- **Access Control Systems**: These systems generate access logs and security footage that can be reviewed to verify access to both physical and digital systems and detect if unauthorized access has occurred.
- **Zero Trust Security**: Like access control systems, zero trust security measures will provide a record of access to digital systems and data. By validating a user's identity at every request for access, zero trust measures provide granular information about access.
- **Chain of Custody**: Chain of custody produces an auditable record of an asset's transfers and transactions, enabling detection of a potential threat if there is a gap in the chain.

Continuous Monitoring

Monitoring for insider threats, as well as for any issues with the systems in place, should be continuous. This involves a combination of human and digital tools, underpinned by a strong organizational culture of proactive reporting. All employees have a part to play in the process to hold themselves and others accountable for following established procedures. Through ongoing, proactive monitoring, even the most organized and well-resourced election office may find practices that are outdated or not consistently followed, leaving the organization exposed to risk if not properly addressed. Finally, all procedures and practices, including any monitoring programs, should be regularly reviewed and updated for compliance with applicable federal, state, and local laws.

Auditing

Internal audits of all election and business processes should be a routine part of election administration before, during, and after an election. Audits validate whether measures such as access control and chain of custody are functioning properly, collecting and maintaining necessary data or equipment, and 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. Audits should be used to look for evidence that demonstrates the effectiveness and durability of procedures, processes, systems, and training practices.

Election infrastructure stakeholders are encouraged to identify a timeline for periodic audits that makes sense for their workflow and capacity; smaller and more frequent internal audits of different processes may be less disruptive than one major year-end audit. It is recommended to build audits into an organization's SOPs. Election infrastructure stakeholders should not wait for external requests to perform audits of their systems and processes.

Transparency

The election process is transparent and open to public observation, which provides a unique strength compared to many other critical infrastructure areas. Allowing the public to assist with and observe the election process can help illuminate points where the process is unclear and provide opportunities to make improvements. From the perspective of insider threats, public participation may result in detecting "false positives" due to lack of clarity or understanding. This underscores the importance of documenting procedures thoroughly, testing and auditing them, and educating the public on them.

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 an insider incident in any of its expressions. The insider threat management team 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 the initial screening of these three questions indicates that there is not an immediate potential for a 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. During the investigation stage, the insider threat management team may need to consider consulting with an external threat assessment professional, consulting with legal counsel, and/or initiating coordination with law enforcement, as necessary.

The purpose of the investigation is to gather evidence (including from 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, assisting with finding outside counseling or support, and/or reporting to law enforcement.

Emergency Intervention

If it is determined that emergency intervention is required based on the initial screening, then the organization should take immediate action, including calling for assistance from first responders or law enforcement if necessary.

In the event of physical violence or sabotage, the team should initiate the organization's Incident Response Plan, skip the initial screening, contact appropriate authorities, and begin an investigation as soon as it is safe to do so. For cases of targeted violence or sabotage, emergency intervention can sometimes result in the need to evacuate a location or facility, initiate a lockdown, or shelter in place. The organization should have plans in place for each response and coordinate across the organization for immediate action.

MANAGING INSIDER THREATS

As discussed above, effective insider threat mitigation requires that organizations foster a positive, supportive culture that encourages employees to report unusual behavior. Integral to this goal is a transparent and consistent process for reporting, where both staff and the public know that their reports will be acknowledged, taken seriously, and handled appropriately. Election infrastructure stakeholders should emphasize that contribution toward this goal is shared by everyone in the community, including staff, vendors, and volunteers involved in administering elections. Programs that encourage early reporting and intervention increase the likelihood that a threat 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. This helps reinforce a culture of engagement and awareness and enables the entire team to be better prepared in the future.

FURTHER RESOURCES

Insider Threat Mitigation

- CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute: Offers written products for insider threat mitigation across a variety of organizational settings.
- I Insider Threat Mitigation Resources | CISA: Shares overarching guidance to aid individuals, organizations, and communities in understanding insider threats and improving or establishing an insider threat mitigation program.
- Insider Threat Mitigation Guide | CISA: Provides comprehensive guidance for organizations of all sizes in support of the establishment or enhancement of an insider threat mitigation program. The information within the guide is scalable and allows for the consideration of the level of maturity and size of the organization.
- Insider Risk Self-Assessment | CISA: A tool to assist owners and operators or organizations, especially small and mid-sized ones who may not have in-house security departments, to gauge their vulnerability to an insider threat incident. The tool is a downloadable PDF that asks users key questions about their existing enterprise, focusing on the domains of Program Management, Personnel and Training, and Data Collection and Analysis.
- National Insider Threat Task Force (NITTF): Helps federal departments and agencies identify best practices for detecting, deterring, and mitigating emerging threats. NITTF also provides a variety of products and resources applicable to state, local, tribal, and territorial and critical infrastructure entities.
- FBI Insider Threat: An Introduction to Detecting and Deterring an Insider Spy: An introduction for managers and security personnel on behavioral indicators, warning signs, and ways to detect and deter insiders from compromising organizational trade secrets and sensitive data more effectively.

Mis-, Dis-, and Malinformation (MDM)

- MDM Resource Library: CISA's Mis-, Dis-, and Malinformation (MDM) team is charged with building national resilience to MDM and foreign influence activities. Through these efforts, CISA helps the American people understand the scope and scale of MDM activities targeting elections and critical infrastructure and enables them to take actions to mitigate associated risks.

Cybersecurity for Critical Infrastructure

- Framework for Improving Critical Infrastructure Cybersecurity | NIST: Provides a framework and path forward for critical infrastructure stakeholders to assess cybersecurity risks, improve risk management, and prioritize and achieve cybersecurity objectives.
- Supply Chain Risk Management Practices for Federal Information Systems and Organizations | NIST: Expands on cybersecurity risk management guidance by diving deeper into information and communications technology (ICT) supply chain risks and how to identify, assess, and mitigate them.

Chain of Custody

- Chain of Custody and Critical Infrastructure Systems | CISA: Overview of what chain of custody is, potential impacts and risks of broken chain of custody, and an initial framework for securing physical and digital assets for those working on critical infrastructure systems.
- Chain of Custody Best Practices | EAC: Best practices in chain of custody practices specifically for election officials.
- Chain of Custody – General Terminology and Models: International Organization for Standardization (ISO 22095:2020) guidance on chain of custody processes.

Conducting Internal Audits

- Unique Aspects of Internal Auditing in the Public Sector | IIA: This guidance will enable internal auditors to plan and perform internal audit engagements with an understanding of the unique roles and principles of public sector organizations.
- Assessing Organizational Governance in the Public Sector | IIA: Overview of how internal auditors can assess and make appropriate recommendations for improving governance activities and processes for public sector organizations.
- Creating an Internal Audit Competency Process for the Public Sector | IIA: This guide helps ensure that an organization's audit function has the collective knowledge, skills, and other competencies necessary to complete planned audits.

Election Technology Procurement

- A Guide for Ensuring Security in Election Technology Procurements | CIS: A guide on procuring computer hardware, software, and services for election administration.
- Managing Cybersecurity Supply Chain Risks in Election Technology | CIS: This guide for election technology providers provides best practices for specific problem areas identified by the election community.