



# 2024 U.S. Federal Elections: The Insider Threat



The Federal Bureau of Investigation (FBI), in coordination with the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Election Assistance Commission (EAC) prepared this overview to help partners defend against insider threat concerns that could materialize during the 2024 election cycle. For years, federal, state, local, and private sector partners nationwide have worked closely together to support state and local officials in safeguarding election infrastructure from cyber, physical, and insider threats. Because of these efforts, there is no evidence that malicious actors changed, altered, or deleted votes or had any impact on the outcome of elections. Over the past several years, the election infrastructure community has experienced multiple instances of election system access control compromises conducted by insider threats. While there is no evidence that malicious actors impacted election outcomes, it is important that election stakeholders at all levels are aware of the risks posed by insider threats and the steps that they can take to identify and mitigate these threats.

This document outlines several recent examples of election security-related insider threats, discusses potential scenarios that could arise during the 2024 election cycle, and provides recommendations for how to mitigate the risk posed by insider threats.<sup>1</sup>

## Insider Threats to Elections

In the United States, elections are administered at the state and local levels of government, which has resulted in a diverse landscape of election systems and technologies across the country. Throughout the election cycle, many people are involved in administering or carrying out responsibilities that support elections, including election workers, officials from other divisions of government, vendors, contractors, temporary workers, and volunteers. Understanding what constitutes insider status and how insiders can present risks to an organization are important components of developing a comprehensive insider threat mitigation program.

An insider threat can be an individual or group who uses their authorized access or special knowledge to cause harm to an organization or entity. This harm can include malicious acts that impact the security and integrity of election systems and information. Insider threats could manifest as current or former employees, temporary workers, volunteers, contractors, or any other individuals with privileged access to election systems and information. This could include individuals who work outside of the immediate election office in roles that support or interact with infrastructure that the election office relies upon.

## Recent Examples of Election Infrastructure-related Insider Threats

- A temporary election worker inserted an unauthorized personal flash drive into an electronic poll book containing voter registration data, including confidential information barred from release under state law. The temporary election worker extracted the data because they wanted to compare it against documents they would acquire after the election through the Freedom of Information Act. The breached election equipment was decommissioned after this incident was identified.

<sup>1</sup> 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](http://www.fbi.gov/contact-us/field)).

- A State identified a series of digital images of a voting system from one of its counties and related confidential passwords published on the Internet without authorization. Further review determined a county clerk and their subordinate allegedly granted an unauthorized person access to the county's voting machines. The clerk and the subordinate also allegedly disabled the security cameras and gave false identifying credentials to the unauthorized individual.
- A county official reported an attempt to gain unauthorized access to the county's election network during the state's spring primary election. According to the official, someone was granted access into a government office where they were able to plug an unauthorized laptop into a government network. Data from that election network later appeared at a public gathering discussing perceived election fraud issues.
- Two county officials allowed unauthorized users access to their election systems during an audit process, resulting in the state's chief election official subsequently decertifying the machines and prohibiting them from being used in future elections.

## Potential for Foreign Adversary Exploitation of Insider Threats

To date, the examples of insider threat activity related to the elections process have been domestic in nature, both in terms of the actor and the motivations. However, since at least 2016, a growing number of foreign adversaries have continued to monitor election networks and attempted to influence or interfere in U.S. elections. While we assess that the threat of a foreign adversary gaining access to election infrastructure through a witting insider is minimal, the perceived normalization (or steady-state) of election influence or interference might help drive some adversaries to push the boundaries of U.S. "red lines," such as targeting and exploiting U.S. persons or election workers to interfere in U.S. elections. One way this foreign derived threat could manifest is via attempts to exploit insider access to interfere with election infrastructure or processes. Foreign adversaries, as well as other malicious actors such as criminal networks, could attempt to gain insider access through a variety of methods.

- Adversaries may seek to gain insider access by exploiting a targeted insider's ideological views, providing financial incentives, or using proxy organizations or diplomatic presence to establish contact with an individual either already in a position of trust or would be willing to seek out and acquire a position on behalf of the foreign actor.
- Adversaries may attempt to blackmail or coerce an insider to leverage the insider's access, collect insights on election security efforts and vulnerabilities, or direct the insider to perform malicious activity. Prior to initiating contact, the foreign adversaries likely would collect information on the target to uncover anything they could use for blackmail or coercion. The type of information could include financial debts, and potentially embarrassing or illegal activity.

In the event an adversary was to gain access to election infrastructure via an insider, they could potentially use that access to disrupt processes and/or spread false information in an attempt to discredit the electoral process and undermine confidence in U.S. democratic institutions.

- If an adversary gained access through an insider to election systems in a particular jurisdiction, such activity could expose voters' personal information, hinder voters' ability to access accurate information on election day or render these systems temporarily inaccessible to the public or election workers, all of which could slow, but would not prevent, voting or the reporting of results.
- In addition, adversaries could also employ insiders to assist with their malign influence operations to undermine American confidence in the security and integrity of the elections process. An insider could provide an adversary with material to develop or amplify messaging challenging election system security, results, or operations. This

includes through coordinated data leaks or the publication of information alleging an adversary's compromise of election infrastructure.

## Potential Indicators of Insider Threat Activity

Individuals at risk of becoming insider threats often exhibit warning signs, or indicators.<sup>2</sup> The following list is not all inclusive, but contains potential flags that election officials should be alert to and seek further review by authorities:

- Attempting to alter or destroy ballots, mail-in ballot envelopes, administrative documentation, or allowing others to access these materials without prior approval.
- Without need or authorization, accessing systems, equipment and/or facilities they have no need to access or providing unauthorized personnel access.
- Turning off security cameras or access control systems or disregarding two-person rule requirements.
- Without need or authorization, taking proprietary or other material home via documents, thumb drives, computer disks, or e-mail. Unnecessarily copying material, especially if it is proprietary or sensitive.
- Remotely accessing the computer network at odd or unexpected times atypical for normal operations.
- Disregarding agency computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Intimidating or threatening other staff.

## Securing Your Organization: Building an Insider Threat Mitigation Program

Election workers 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 (often bipartisan), to robust chain-of-custody procedures, to the presence of observers during voting and ballot 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.

Organizational culture should also 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 or requiring the “buddy system” or a two-person minimum for handling sensitive tasks. Checklists are helpful tools for promoting adherence to SOPs.

<sup>2</sup> (U) The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy | FBI | 21 May 2016 | [https://www.fbi.gov/file-repository/insider\\_threat\\_brochure.pdf/view](https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view)

- Physical and Digital Access Control** systems can detect and prevent insider threats. Access control systems 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, as well as 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.
- A key challenge around access control for election workers is access to the state voter registration database system. The state may not always 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.
- 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 for it. This can help prevent unauthorized access to sensitive systems, detect the presence of an insider threat, provide evidence, and improve remediation time if an incident occurs. It 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.
  - Zero Trust 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. 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 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.
  - Continuous Monitoring** is a key practice for detecting anomalous behavior, to include potential insider threats. It involves a combination of the human and digital tools—such as access logs, video surveillance, endpoint detection and response software—underpinned by a strong organizational culture of proactive reporting.
  - Auditing** 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, 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. It is recommended to build audits into an organization’s SOPs.
  - Follow Cybersecurity Best Practices** for systems and networks to implement a defense-in-depth approach that prevents single points of failure from being enough for a system compromise. These security best practices are also designed with the expectation that a malicious actor has already obtained access to a like system or software to try and identify vulnerabilities. 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.

- **Reporting** all incidents to the appropriate authorities so they can be investigated and documented can prevent or reduce the likelihood of similar incidents occurring in the future.

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. To assist stakeholders with their insider threat mitigation efforts, CISA developed an “Insider Threat Reporting Template” and an “Insider Threat Investigation Template” as tools for organizations to download, review, and incorporate into their insider threat mitigation programs. These templates and “Insider Threat Reporting Templates User Guide” are annexes to this guide and can be found on the CISA #PROTECT2024 website and are linked below.

## Additional Election Security Resources and Contacts

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](http://www.fbi.gov/contact-us/field)).

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

- [Protected Voices – FBI](#)
- [#Protect2024 - CISA](#)
- [Election Security – U.S. Election Assistance Commission \(eac.gov\)](http://eac.gov)
- [Election Security - Dept of Homeland Security](#)
- [Election Crimes and Security – FBI](#)



# Insider Threat Reporting Templates

The Cybersecurity and Infrastructure Security Agency (CISA) created these reporting templates as a tool for stakeholder organizations to download, review, and incorporate into their insider threat mitigation programs. The **Reporting Form** and the **Investigative Form** are fillable PDFs that can be used with any insider threat program. Like other templates CISA has developed, stakeholders can utilize the forms in their current format or use them as an example in developing their own products internally.

The **Reporting Form** allows individuals to submit concerns related to a potential insider threat to the appropriate point of contact within their organization. This form features a “submit” button that organizations can edit to auto-generate an email to the appropriate mailing address within the organization. An organization intending to use the Reporting Form will need to edit the “submit” button as outlined in this document before making the form available for employee use. This helps ensure that all reports are collected centrally by the appropriate selected recipient(s) or inbox.

The **Investigative Form** is designed to help organizations document incidents and determine appropriate next steps, including, but not limited to, review by an organization’s Threat Management Team, referral to law enforcement, or other follow-on actions as necessary to protect the organization and its employees. This will assist stakeholders as they keep a record of organizational actions related to an insider threat incident, promote accountability of necessary steps to protect assets, and to identify vulnerabilities in the effort of mitigating future insider threats.



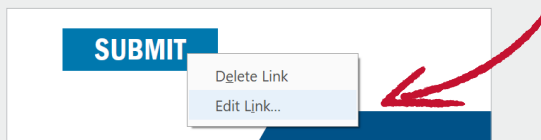
**The forms are downloadable and the data collected is controlled and managed by the policies and protocols of the stakeholder organizations.**



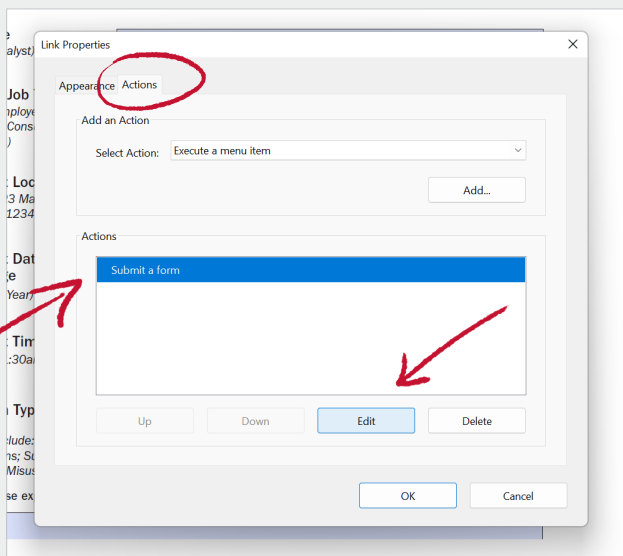
**If you have a concern about an immediate threat in the workplace, contact your local law enforcement.** The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

## EDITING THE REPORTING FORM FOR YOUR SPECIFIC ORGANIZATION:

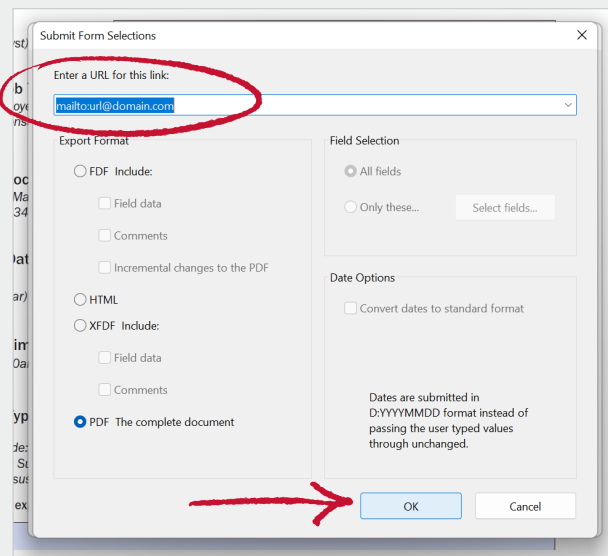
1. Right-click **SUBMIT** button and click “Edit Link...”



2. Navigate to “Actions” tab and edit the “Submit a form” action



3. Edit the “mailto:url@domain.com” line to your preferred email address and click OK



# Insider Threat Reporting Template

## WORKPLACE REPORTING FORM

The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

**Please use this section to report any suspicious activity in the workplace, focusing on documenting the incident and providing relevant details about the observed behavior/incident:**

1 | Description of Incident

*Provide as many details as you can regarding the incident and your observations.*

2 | Incident Location

*Example: 123 Main Street, Anytown, ST 12345*

3 | Incident Date or Date Range

4 | Incident Time(s)

*Example: 11:30 A.M.*

5 | Concern Type

*Examples include: Verbal/Written Threats; Terrorism/Violent Extremism; Personal Conduct; Financial Considerations; Substance Abuse; Behavioral Considerations; Criminal Conduct; Mishandling Protected Information; Misuse of Information Technology; Cyber Crime; Espionage; Financial/Intellectual Property Theft; Workplace Violence*

**Please share details about the individual(s) associated with the suspicious activity in the following section:**

6 | Name (or Description if Unknown)

*Example: John Doe*

7 | Job Title

*Example: Analyst, Sales Rep, Software Engineer*

8 | Role or Job Type

*Example: Employee, Contractor, Consultant, Vendor, etc.*

*This reporting template is intended to document activities and behaviors that are suspicious or indicative of criminal activity. Such activities or behaviors should be reported only when there are articulable facts to support a rational conclusion that the behavior is suspicious or suggests criminal activity. Do not report based on constitutionally protected activities or on the basis of race, ethnicity, religion, gender, sexual orientation, disability, or other such characteristics, and do not report based on a combination of only such factors. **If you have a concern about an immediate threat in the workplace, contact your local law enforcement.***

**SUBMIT**

# Insider Threat Reporting Template

## WORKPLACE INVESTIGATIVE FORM

REPORT NUMBER

The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

### INCIDENT DETAILS

1	<b>Incident Description</b>	<i>Outline incident in further detail (i.e. witness statement, etc.). What IT systems were compromised? What technology identified the breach (if applicable)?</i>		
2	<b>Concern Type</b>	<i>Examples include: Verbal/Written Threats; Terrorism/Violent Extremism; Personal Conduct; Financial Considerations; Substance Abuse; Behavioral Considerations; Criminal Conduct; Mishandling Protected Information; Misuse of Information Technology; Espionage; Financial/Intellectual Property Theft; Other</i>		
3	<b>Has the appropriate security professional been notified?</b>	<i>Yes</i>	<i>No</i>	<i>N/A</i>
4	<b>Has the Insider Threat Management Team been notified?</b>	<i>Yes</i>	<i>No</i>	<i>N/A</i>

### INFORMATION ON THE PERSON OF INTEREST

5	Name	
6	Job Title	
7	Labor Category	
8	Clearance Level /Special Access	
9	Network Privileges	
10	Equipment Used in Incident	
11	Office Location	
12	Incident Date or Date Range	
13	Incident Time(s)	

### INVESTIGATOR/INTAKE OFFICIAL'S INFORMATION

14	Name	
15	Contact Information	
16	Position	



## ADDITIONAL INFORMATION

- 17 **Initial Recommendations** *Does law enforcement need to be involved? What action needs to occur to keep individuals safe?*
- 18 **How was the suspicious activity detected?** *What activity occurred? What was the individual's main motivation (if known)? Were any organizational policies violated? How were the security policies/procedures evaded if possible? What action did the organization take to mitigate and prevent an incident?*
- 19 **Next Steps, Follow-up, and Conclusion** *What actions did the organization take? Were consequences for the individual recommended to HR such as a formal warning, suggested counseling, or termination? Was the matter sent to law enforcement for further investigation? Were witness interviews conducted? What action must come next in this particular instance?*
- 20 **Recommendations / Updates / Changes to Make** *What security considerations should the organization address? What changes need to be made to protect the organization's high-value assets? Did the reporting pathway lead to a successful mitigation or prevention? If not, what security gap needs to be addressed? Is increased monitoring of the individual needed?*

## REPORT REVIEWED BY

Name

Title

Law Enforcement Investigation Number (if applicable)

Investigating Office (if applicable)

Date