CISA
CYBER+INFRASTRUCTURE

Insider Threat Programs for the Critical Manufacturing Sector

Implementation Guide

August 2019

This page intentionally left blank.

Letter from the Assistant Director and the Director

Threats from trusted insiders with authorized access to an organization can wittingly or unwittingly harm that organization, its resources, and disrupt operations. Unmitigated insider risk can increase the danger of attack on an organization.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) works closely with the Critical Manufacturing Sector to improve the sector's security and resilience. The Department of Defense's Defense Counterintelligence and Security Agency supports cleared facilities' efforts to protect classified information. Both agencies' missions involve creating resources to help organizations protect against insider threats.

The *Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide* was developed to provide guidance and information for critical manufacturing organizations to establish insider threat programs. These programs serve to gather, monitor, and assess information for insider threat detection and mitigation strategies. Insider threat programs are designed to detect, deter, and mitigate the risks associated with trusted insiders and protect the privacy of the workforce while reducing potential harm to the organization. Effective insider threat programs deploy risk management strategies that identify the assets or resources to be protected, identify potential threats, determine vulnerabilities, assess risk, and deploy countermeasures.

CISA and DCSA appreciate the participation and dedication in developing this guide of Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) members along with members of our private sector. A more protected Critical Manufacturing Sector from insider threats is a stronger sector.

As CISA's Assistant Director for Infrastructure Security and DCSA's Director of the Center for Development of Security Excellence, we encourage you to use and reference this Guide. Thank you for your partnership and commitment to securing our nation.

Sincerely,

Brian Harrell
Assistant Director for Infrastructure Security

Kevin Jones
Director of the Center for Development of Security Excellence

This page intentionally left blank.

Trusted insiders, both witting and unwitting, can cause grave harm to your organizations, facilities, resources, and personnel. Insider incidents account for billions of dollars annually in "actual" and "potential" lost revenue related to trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more. Insider threat programs can mitigate risks associated with trusted insiders. Click the links to learn how to establish an insider threat program at your organization and develop a risk management strategy that addresses areas critical to manufacturing.

Understanding the Insider Threat

Page 3

Establishing an Insider Threat Program

Page 5

Insider Risk Management Strategy

Page 9

Insider Threat Program Resources

Page 13

1 Understanding the Insider Threat

What is an Insider Threat?

Anyone with authorized access who uses that access to wittingly or unwittingly harm the organization and its resources. Insiders can include employees, vendors, partners, suppliers, and others to whom you provide access to your facilities and/or information. Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many risks can be mitigated before harm to the organization occurs. Learn more about insider threat indicators and find free training and awareness materials at https://www.cdse.edu/toolkits/insider/index.php.

What Risks Do Insider Threats Pose to Critical Manufacturing?

Numerous threats have the potential to cause major disruption in manufacturing operations. These include malicious acts committed by insiders such as fraud, theft, sabotage, workplace violence, and more. Unwitting insiders may inadvertently disclose proprietary or other sensitive information, unknowingly download malware, or facilitate other cybersecurity events. The critical manufacturing sector reports the highest number of attacks on industrial control systems of any critical infrastructure sector. Unmitigated insider risk is likely to increase the risk of attack. See the case study at right or visit https://www.cdse.edu/resources/case-studies.html for more real-world events.

Why Establish an Insider Threat Program?

Insider threat programs are designed to detect, deter, and mitigate the risks associated with trusted insiders. Multidisciplinary teams comprised of security, human resources, cyber/information technology (IT), legal, and other professionals from throughout your organization gather, integrate, and assess information indicative of potential risk and determine appropriate mitigation response options on a case-by-case basis. Insider threat programs protect the privacy of the workforce while reducing potential harm to the organization. See the Establishing an Insider Threat Program section on page 5 to learn more.

What Can My Organization Do to Reduce the Risk Associated with Trusted Insiders?

Effective insider threat programs deploy risk management strategies that identify the assets or resources to be protected, identify potential threats, determine vulnerabilities, assess risk, and deploy countermeasures. Many countermeasures are no or low cost to the organization and include training and awareness, clear reporting policies, managing organizational trust, and enhanced security procedures. Review the Insider Risk Management Strategy on page 9 to learn more.

What Resources are Available to Me?

The Department of Homeland Security, Department of Defense, National Insider Threat Task Force, Federal Bureau of Investigation, and National Counterintelligence and Security Center have numerous free resources available to your organization. Review the Resources section on page 13 to learn more.

Wen Chyu Liu

While employed at a major manufacturing company, Liu worked as a research scientist on various elastomer products. Liu conspired with at least four current and former employees to steal elastomer trade secrets and sell them in China. The company lost valuable research that impacted numerous projects. Long-held trade secrets were disclosed to competitors and the public and profits from current and future projects were compromised. Numerous employees were fired and several prosecuted. Read the full case study at https://www.cdse.edu/documents/cdse/wen-chyu-liu.pdf.

2 Establishing an Insider Threat Program

Setting Up Your Program

An insider threat program is a multidisciplinary activity established by an organization to gather, monitor, and assess information for insider threat detection and mitigation. Program personnel analyze information and activity indicative of an insider risk and determine appropriate mitigation response options up to and including referral to the appropriate officials for investigation and/or resolution. Best practices encourage the insider threat program to include a multidisciplinary team consisting of Legal Counsel, Security, Counterintelligence, Cybersecurity, Mental Health and Behavioral Science, and Human Resources or Human Capital disciplines to effectively counter insider threats to your organization. The exact makeup of your insider threat program will depend on the size and complexity of your organization.

Insider threat programs take proactive measures to **deter, detect, mitigate, and report the threats** associated with trusted insiders. The program identifies anomalous behaviors that may indicate an individual poses a risk. Early identification allows insider threat program personnel to focus on an individual's issues of concern or stressors and deploy appropriate mitigation responses. When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and reports information outside the organization as required.

The first step in establishing your program is to **identify the program office and leadership**. You must determine how the team will be structured and where it will be located. Does your organization have the ability to house the team in a single location? Or are the team members geographically separated and must rely on virtual communications to conduct operations? Your organization should select an insider threat program senior leader or program manager who oversees day-to-day operations. They will work with the organization's senior leadership to determine resource and staffing needs.

You should **establish rules for how the insider threat program will operate** within your organization. As part of rule and policy development, the insider threat program should also identify practices for safeguarding sensitive personnel information along with consequences for violations of internal rules committed by insider threat program team members. Insider threat team members must maintain standards of professional conduct like any other personnel. However, because you're dealing with extremely sensitive information it's important that you clarify these responsibilities up front. A sample insider threat program plan is included in the Resources section.

You should also **ensure that insider threat program personnel are properly trained** to conduct their duties. Insider threat program personnel must be able to appropriately respond to incident reporting, protect privacy and civil liberties, support mitigation options, and refer matters as required. Many free training options exist. Consult the Resources section on page 13 for more information.

Detecting and Deterring Insider Threats

The purpose of an insider threat program is to proactively deter, detect, mitigate, and report threats associated with trusted insiders. These actions make up your daily operations. Insider threat programs detect individuals at risk of becoming insider threats by identifying potential risk indicators. These observable and reportable behaviors or activities may indicate an individual is at greater risk of becoming a threat. Insider threat hubs deter potential insider threats by instituting appropriate security countermeasures, including awareness programs.

Training and Awareness Programs. You must train and exercise your workforce to recognize and report potential risk indicators. It is a best practice to require personnel to complete initial and annual insider threat awareness training. You can also maintain workforce awareness of insider threats and employee reporting responsibilities year-round by instituting a vigilance campaign. Insider threat programs can also conduct internal evaluations. These are small exercises used to test your workforce's knowledge of insider threat indicators and reporting requirements. These exercises do not have to be elaborate but should help you gauge the effectiveness of your program. You may use information from these evaluations to adjust your training and awareness program to ensure effectiveness. See the Resources section on page 13 for access to free training and awareness materials.

Reporting Procedures. Your insider threat program must establish reporting procedures for the general workforce. Those who witness potential indicators should know exactly when, where, and how they can report the information. Prepare procedures for "walk-ins" or those who may want to report their information face to face. Procedures should also include hotlines or dedicated email addresses. Individuals should be encouraged to self-report any issues they may be experiencing. One of the goals of an insider threat program is to deter adverse actions by pointing those asking for assistance to resources that can help them. The challenge is to have people see the insider threat program as a resource rather than a punitive element. You can build this rapport by informing the workforce of your program, the mission, and its goals; by respecting privacy and civil liberties; and by deploying appropriate insider threat mitigation responses.

Organizational Justice. As a best practice, insider threat programs should consider the concept of organizational justice. Organizational justice refers to employee perceptions of fairness in the workplace. Labor relations can have an overall effect on the number of insider threat incidents you see. The worse the labor relations are, the more incidents you may encounter. Counterproductive workplace environments have consequences that can lead to disgruntlement. Organizational leadership that develops a positive workplace environment keeps the workforce engaged and productive. This same concept applies to the insider threat program. Ensuring appropriate mitigation response options and the protection of privacy and civil liberties in the conduct of your duties will minimize negative outcomes from maladaptive responses. Being responsive to workforce concerns is a great way to build rapport with personnel; encourage future reporting; and ultimately mitigate risk.

Instituting User Activity Monitoring

User Activity Monitoring (UAM) is the technical capability to observe and record the actions and activities of an individual operating on your computer networks to detect potential risk indicators and to support mitigation responses. Logging, monitoring, and auditing of information system activities can lead to early discovery and mitigation of behavior indicative of insider threat. UAM also plays a key role in prevention, assistance, and response to acts of violence. As such, UAM development should include consideration of potential acts of violence against organizational resources, including suicidal ideation.

Implementation will be specific to your location, but as a best practice your organizations should:

- Define what will be monitored
- Indicate how monitoring will be instituted
- Inform users of monitoring actions via banners
- Identify indicators that require review (e.g., trigger words, activities)
- Protect user activity monitoring methods and results
- Develop a process for verification and review of potential issues
- Establish referral and reporting procedures

Establishing baseline user behaviors will make deviations or anomalies stand out from normal activities. It will also help determine what your user activity monitoring triggers, also known as internal security controls, should be. Once a "Normal

Activity" baseline is established, internal security controls help us identify deviations. For example, user activity monitoring could help identify a rash of IT system misuses that suggest an employee needs some re-training. Another example would be access control logs indicating an employee is working irregular hours or has unexplained absences from work. UAM can help identify potential risk indicators that can be evaluated during your risk management and mitigation process.

For more information, access the Insider Threat Indicators in User Activity Monitoring job aid at https://www.cdse.edu/documents/cdse/Insider-Threat-Indicators-in-UAM.pdf.

Now that you've established an insider threat program, it's time to employ risk management and mitigation strategies. Your insider threat program should be able to identify and mitigate many issues before they escalate into negative behavior and respond appropriately when preventative actions are not feasible. Access the Insider Risk Management Strategy section on page 9 to learn more.

3 Insider Risk Management Strategy

Risk Analysis

Risk-based analysis allows the insider threat program to manage risk in a complex threat environment. The process of identifying assets, assessing threats and vulnerabilities, evaluating risk, and identifying countermeasures can help **determine the risks most closely associated with trusted insiders in the critical manufacturing sector** and the best methods to deter and mitigate them. It also allows your organization to differentiate between exigent threats to your enterprise and less pressing matters.

Identify Critical Assets

The most basic function of an insider threat program is to protect the assets that provide your organization with a competitive advantage. According to ISO 55000, **an asset is something with potential value to an organization** and for which the organization has a responsibility (Riso 2012). We further elaborate on this definition by stating that a critical asset can be thought of as something of value that, if destroyed, altered, or otherwise degraded, would impact the confidentiality, integrity, or availability and have a severe negative effect on the ability of the organization to support essential missions and business functions.

Critical assets can be both physical and logical and can include facilities, systems, equipment, and technology. An often overlooked aspect of critical assets is intellectual property. This may include proprietary software, customer data for vendors, schematics, and internal manufacturing processes. The organization must keep a close watch on where data is at rest and in transport. Current technology allows more seamless collaboration than ever, but also allows the organization's sensitive information to be easily removed from the organization.

A complete understanding of critical assets (both physical and logical) is invaluable in defending against attackers who will often target the organization's critical assets. The following questions help the organization to identify and prioritize the protection of its critical assets:

- What critical assets do we have?
- Do we know the current state of each critical asset?
- Do we understand the importance of each critical asset and explain why it is critical to our organization?
- Can we prioritize our list of critical assets?
- Do we have the authority, money, and resources to effectively monitor our critical assets?

The role of the program manager is to work with all of those across all areas of the organization to answer the questions above. Once those questions are answered within each division, input from senior-level management should be obtained to prioritize protection across the organization. Once critical assets are **identified and prioritized, the organization must identify those high-risk users who most often interact with the critical systems or data**. This will help the organization to identify the best approaches to successfully identify potential insider threats.

Conducting a Risk Assessment

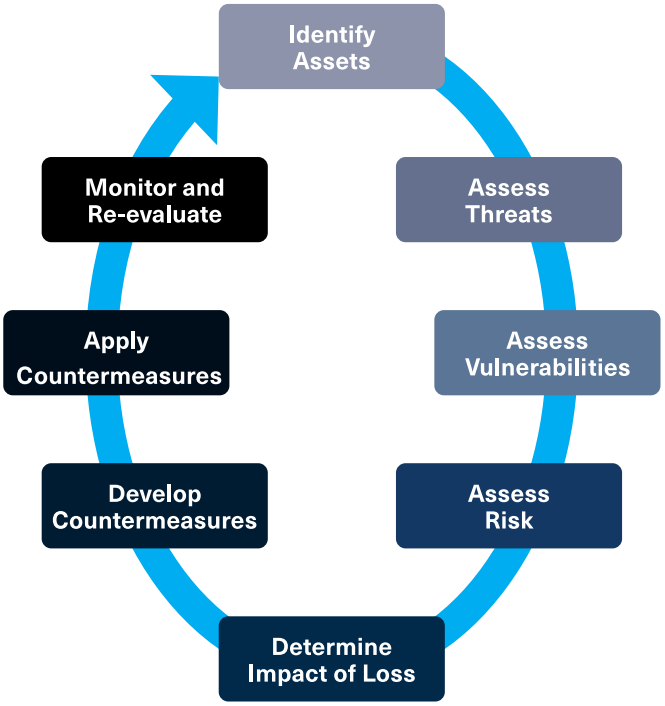
The Risk Management Process

Risk management is an eight step process that provides a framework for collecting and evaluating information to:

- Identify assets (identify value of asset)
- Assess threats (intent and capability of adversaries)
- Assess vulnerabilities (identification and extent of vulnerabilities)
- Assess risk (determine the likelihood that a threat will exploit your vulnerabilities)
- Determine impact of loss, damage, or compromise of asset

- Develop countermeasures (security countermeasure options that can reduce or mitigate risks cost effectively)
- Apply countermeasures
- Monitor and re-evaluate

For more information on risk management, visit https://www.cdse.edu/catalog/elearning/GS150.html.



One of the major difficulties facing organizations is being able to rank and score accurately the different critical assets provided to the decision-makers. Our experience shows us that many stakeholders within an organization will often state "the asset they know about and control" is in their opinion the most critical. Instead of providing subjective and biased ranking of critical assets, we suggest using various metrics and discussing them internally with various employees of the organization.

When attempting to rank and score the potential pool of critical assets, we suggest leveraging a statistical tool known as Pairwise Rankings. This approach will essentially allow a group to perform the ranking by comparing two critical assets at a time and giving each a numerical rating. The numerical ratings are then added up and sorted in ascending order to show the most critical asset.

You may also consider implementing the Risk Management Framework (RMF) for information systems. More information on RMF is available from the National Institute of Standards and Technology at https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview. You can also access free training on the topic at https://www.cdse.edu/catalog/elearning/CS124.html.

Risk Mitigation

To be effective, insider threat programs must be on the lookout for potential issues before they pose a threat. In most cases, **proactive mitigation responses provide positive outcomes for both the organization and the individual**. This allows you to protect information, facilities, and personnel and retain valuable employees as well as offers intervention to help alleviate the individual's stressors.

Your insider threat programs responses are situationally dependent, but may include recommendations such as:

- Suspending access to information
- Taking personnel actions such as counseling, referral, or termination
- Organizational responses that may require changes to policy or procedures
- Increased or additional training

Human Resources insider threat program team members can assist with counseling referrals or prescribed human resource interventions that may be corrective in nature. They deal with Employee Assistance Programs for resources in financial counseling, lending programs, mental health, and other well-being programs.

Insider threat program team members from the various security disciplines, whether cyber/IT, personnel, information, or physical, can assist with mitigation response options such as updating security protocols, adjusting UAM or other inspections, and providing basic security training and awareness to the workforce. **Some insider threat incidents may warrant external referrals to counterintelligence or law enforcement authorities**. Have a plan in place for referring

these actions and consult with your legal counsel to ensure that proper protocols are followed.

Your program should **create a record of the incident outcome**. You may also create or coordinate with other elements within your organization to develop a "Damage Assessment" or "After Action" Report that explains the damage to the organization, personnel, facilities, or other resources. You may need to work with the legal team and any other contributing elements to ensure the report is stored and retained appropriately. A sample Memorandum of Activity Report is included in the Resources section on page 19.

4 Insider Threat Resources

Sample Forms

- Insider Threat Program Plan (Page 18)
- Insider Threat Program Memorandum of Activity (Page 19)

Training for Insider Threat Programs

- CDSE - https://www.cdse.edu/catalog/insider-threat.html
- DHS - https://www.dhs.gov/training-awareness

Awareness Materials

- https://www.cdse.edu/toolkits/insider/vigilance.html

Case Studies

- https://www.cdse.edu/resources/case-studies.html

Policies and Best Practices

- https://www.cdse.edu/toolkits/insider/index.php

Supporting Organizations

- Department of Homeland Security—https://www.dhs.gov/insider-threat-mitigation
- National Insider Threat Task Force—https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- Defense Counterintelligence and Security Agency—http://www.dss.mil/
- Center for Development of Security Excellence—CDSE
- Federal Bureau of Investigation—https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view

Critical Manufacturing Sector-Specific Agency Contacts

- Email: criticalmanufacturing@cisa.dhs.gov
- Website: https://www.dhs.gov/cisa/critical-manufacturing-sector

Glossary: Insider Threat Case Studies

CASE STUDY

DDoS attack at a medical facility via HVAC

A hospital facility employed the insider, a contractor, as a security guard. The insider was extensively involved with the Internet underground and was the leader of a hacking group. The insider worked for the victim organization only at night and was unsupervised. The majority of the insider's unauthorized activities involved a heating, ventilation, and air conditioning (HVAC) computer. This HVAC computer was located in a locked room, but the insider used his security key to obtain physical access to the computer. The insider remotely accessed the HVAC computer five times over a two-day period. In addition, the insider accessed a nurses' station computer, which was connected to all of the victim organization's computers and stored medical records and patient billing information. The insider used various methods to attack the organization, including password-cracking programs and a botnet. The insider's malicious activities caused the HVAC system to become unstable, which eventually led to a one-hour outage. The insider and elements of the Internet underground were planning to use the organization's computer systems to conduct a distributed-denial-of-service (DDoS) attack against an unknown target. A security researcher discovered the insider's online activities. The insider was convicted, ordered to pay $31,000 restitution, and sentenced to nine years and two months of imprisonment followed by three years of supervised release.

This case illustrates how a single computer system can cause a great amount of damage to an organization. In this case, the damage could have been life threatening because the attack took place at a hospital facility. Modifying the HVAC system controls and altering the organization's environment could have affected temperature-sensitive drugs and supplies and patients who were susceptible to temperature changes. With additional steps to bypass security, the insider could have potentially modified and impaired patient records, affecting treatment, diagnoses, and care. It is critical that management and information security teams work with other departments within an organization to identify critical systems. In this case, the HVAC computer was located in a locked room, not a data center or server room, which would have afforded the system additional protections and may have prevented the insider from manipulating the system.

In addition, the insider was able to access a nurses' station computer, which had access to other critical organizational systems. If the organization had fully understood the potential impact a compromised workstation could have on other parts of the organization, it could have implemented additional layers of protection that would have prevented this type of attack.

CASE STUDY

Insider Intellectual Property Theft

A chemical manufacturing company employed a senior research scientist working on a multi-million-dollar project related to chemicals used in the production of a new electronic technology. During the month after this insider announced his resignation, he emailed a document detailing the proprietary chemical procedure to his account at the beneficiary organization. After the victim organization examined his company laptop and returned it, he downloaded more than 500 documents from the laptop to an external storage device. Even though the organization consistently responded to requests to transfer data (indicating that the transfer required approval), the insider asked the IT department how to perform the transfer and falsely stated that it had been approved.

In addition to observing the insider's behavioral indicators and suspicious activities, the victim organization had procedures in place to review and approve any transfer of information from company computers. The victim organization also tracked download activity on a regular basis and performed a forensic examination on the insider's computer, a standard practice for transferring employees.

The victim organization's mitigation actions in place, such as approval requirements prior to transferring data, illuminated the insider's suspicious behavior in repeatedly inquiring about transferring data to the victim organization's foreign branch. The reporting and investigating mechanisms enabled the company to identify the suspicious activity and confront the insider about downloading confidential documents and his connection to the beneficiary organization. Further investigation discovered that he copied the documents to his personal computer, with evidence that he transferred information to his personal online email account. The victim organization was able to detect and investigate the incident before the information could be shared with the beneficiary organization.

CASE STUDY

Awareness in Action

Wen Chyu Liu

- Research Scientist 1965-1992
- Age at Conviction: 75
- Conviction Date: 7 February 2011
- Charges: Conspiracy to Commit Trade Secret Theft
- Sentence: Two years supervised release, forfeit of $500K, and $25K fine

Espionage Indicators

- Unexplained Affluence
- Foreign Contracts
- Foreign Travel
- Access to Information Outside Need to Know

What Happened

- While employed at a major chemical manufacturing company, Liu worked as a research scientist on various consumer products.
- Liu conspired with at least four current and former employees to steal elastomer trade secrets and sell them in China.
- Liu traveled extensively throughout China to market the stolen information.
- Liu paid current and former employees for information.
- Liu bribed one current employee with $50,000 in cash for a technical manual.

Impacts

- The company lost valuable research that impacted numerous projects.
- Long-held trade secrets were disclosed to competitors and the public.
- Profits from current and future projects were compromised.
- Numerous employees were fired and several prosecuted.

Learn More

This case study examined a real-life insider threat. Your awareness is key to protecting our national security from insider threats like this one. Visit the Center for Development of Security Excellence's website (http://www.cdse.edu) for additional case studies, information, materials, and training; you can also go directly to the Insider Threat Toolkit at http://CDSE.edu/toolkits/insider/index.php.

If you SEE Something, SAY Something.™

Sample Insider Threat Program Plan for _____

1. Purpose. This plan establishes policy and assigns responsibilities for the Insider Threat Program (ITP).

The ITP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. An insider threat is defined as the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to an organization and its resources. Insider threats may include harm to the organization's information, personnel, and facilities.

The program will gather, integrate, and report relevant and credible information indicative of potential insider risk indicators; deter insider threats; and detect risks posed by those with authorized access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems. The program will proactively mitigate the risk of an insider threat as defined above.

2. Scope and applicability. This Insider Threat Program Plan applies to all staff offices, regions, and personnel with access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems.

3. Guiding Principles.

a. **[Organization name]** is subject to insider threats and will take actions to mitigate or eliminate those threats.

b. **[Organization name]** will continually identify and assess threats to the organization and its personnel and institute programs to defeat
the threats.

4. Policy.

a. The ITP will be established to protect personnel, facilities, and automated systems from insider threats. This program will seek to prevent theft, fraud, sabotage, acts of violence, and the loss of intellectual property, proprietary information, or other sensitive information. The program will actively deter trusted insiders from becoming insider threats. The program will establish the capability to detect insiders who pose a risk to information systems and information. The program will mitigate risks to the organization through administrative actions, referrals to law enforcement as appropriate, or other responses.

b. The ITP will follow identified best practices for insider threat programs and abide by the laws, policies, and regulations of local, state, and federal governments as appropriate.

c. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The ITP will consult with records management and legal counsel to ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.

5. Responsibilities.

a. Insider Threat Program Senior Official (ITPSO) will be designated in writing and will act as the company's representative for ITP-implementing activities.

b. The ITPSO will be responsible for daily operations, management, and ensuring compliance with the organizational policy.

c. Establish an Insider Threat Program based on the organization's size and operations.

d. Provide Insider Threat training for Insider Threat Program personnel and awareness training for the general workforce.

e. Establish user activity monitoring in order to detect activity indicative of insider threat behavior.

f. Establish procedures to access, gather, integrate, and provide for reporting of relevant and credible information across the organization (e.g., human resources, security, information assurance, and legal review) indicative of a potential or actual insider threat to deter, detect, and mitigate the risks of insider threats.

g. Oversee the collection, analysis, and reporting of information across the organization to support the identification and assessment of insider threats.

h. Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the Senior Management.

Administrator Signature _____ **Date** _____

This plan is a sample only and must be tailored to the specific Insider Threat Program procedures and processes in place at your organization.

Insider Threat Program Memorandum of Activity

Inquiry Number:	Reporting Date:	Source of Information:
Dates of Activity:	Date Report Drafted:	Location of Activity:
Type of Activity:	Subject of Inquiry:	Signature:

ACTION: Insider threat program manager (NAME)
received a report from (NAME OF REPORTER)
regarding (NAME OF SUBJECT) .

The report was made to the Insider Threat Program based on the following:

The Insider Threat Program will take the following actions: Coordinate/assess this referral with the Insider Threat Hub team.

OUTCOME/NEXT STEPS:

CISA
CYBER+INFRASTRUCTURE