Insider Risk Mitigation Programs
Food and Agriculture Sector Implementation Guide

As a member of the Food and Agriculture Sector, you play a significant role in national security by protecting public health and safety, the nation, and its economy from contamination, economic espionage, food adulteration, and terrorism.

Trusted insiders, both witting and unwitting, can cause grave harm to your organization's facilities; resources including raw materials, finished products, and information; brand, reputation, and personnel. Insider incidents account for billions of dollars annually in actual and potential damages related to food safety, food defense, tampering, terrorism, trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

Implementation of an Insider Risk Mitigation Program can help address risks associated with trusted insiders. Click the links to learn how to establish an Insider Risk Program at your organization and develop a risk management strategy that addresses areas critical to food and agriculture.

Understanding Insider Risks

Establishing an Insider Risk Program

Insider Risk Management Strategy

Insider Risk Program Resources

CDSE Center for Development of Security Excellence

UNDERSTANDING INSIDER RISKS

WHAT IS INSIDER THREAT?

An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm the organization or its resources. Insiders can include employees, vendors, partners, suppliers and others that 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 threats can be mitigated before harm to the organization occurs. Learn more about insider risk indicators and find free training and awareness materials **here**.

WHAT THREATS DO INSIDERS POSE TO FOOD AND AGRICULTURE?

Numerous threats have the potential to cause major disruption in food and agriculture operations and to harm public health and safety. These include malicious acts committed by insiders such as deliberate food adulteration, fraud, theft, sabotage, and workplace violence. Unwitting insiders may inadvertently disclose proprietary or sensitive information, impact food safety through negligent actions, or unknowingly download malware or facilitate other cybersecurity events. The food and agriculture sector is also vulnerable to transportation and supply chain failures, contamination, and threats to industrial control systems or other technical systems. Unmitigated insider risk is likely to increase these vulnerabilities. Click **here** to learn about real world insider incidents in the food and agriculture sector.

WHY ESTABLISH AN INSIDER RISK MITIGATION PROGRAM?

Insider Risk Mitigation Programs are designed to detect, deter, and mitigate the risks associated with trusted insiders. Multidisciplinary teams or "hubs" are comprised of security, human resources, cyber, legal and other professionals such as quality control, facilities, and employee health and safety from throughout your organization. These teams work together to gather, integrate, and assess information indicative of potential risk and determine appropriate mitigation response options on a case by case basis. Most of these responses allow individuals to retain their position and receive assistance while protecting the organization and its assets. Insider Risk Programs also protect the privacy of the workforce while reducing potential harm to the organization. See the **Establishing an Insider Risk Program** section to learn more.

HOW CAN MY ORGANIZATION MANAGE INSIDER RISK?

Effective Insider Risk Programs deploy risk management strategies that identify the assets or resources to be protected, identify potential threats, determine vulnerabilities, assess risk and deploy countermeasures to mitigate risk. 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** to learn more.

WHAT RESOURCES ARE AVAILABLE TO ME?

The US Department of Agriculture, Food and Drug Administration, Defense Counterintelligence and Security Agency, Department of Homeland Security, National Insider Threat Task Force, Federal Bureau of Investigation, and the National Counterintelligence and Security Center have numerous free resources. View **Insider Risk Resources** to learn more.

Food industry Industrial Control Systems may be distinctly vulnerable to cyber Insider Threats*

"Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing," by the University of Minnesota's Food Protection and Defense Institute illustrates the mounting cybersecurity risk facing the food industry and specific industrial control system vulnerabilities related to networks, USB drives, and aging systems reliant on single points of failure. These systems are particularly susceptible to actions by malicious insiders. Food industry ICS are also at risk from unintentional actions and negligence on the part of employees. Read the full report here.

RETURN TO MAIN PAGE

ESTABLISHING AN INSIDER RISK PROGRAM

SETTING UP YOUR PROGRAM

- **An Insider Risk Mitigation Program is a multi-disciplinary activity or "hub"** established by an organization to gather, monitor, and assess information for insider risk detection and mitigation. Program personnel analyze information and activity indicative of 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 Risk Program to include a multidisciplinary team consisting of Legal Counsel, Security, Cybersecurity, Mental Health and Behavioral Science, and Human Resources or Human Capital disciplines to effectively counter insider risks in your organization. The exact makeup of your Insider Risk Program will depend on the size and complexity of your organization. Consult the **Quick Start Guide** for step-by-step recommendations.

- Insider Risk Mitgation 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 Risk 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 Risk Mitigation Program Senior Leader or program manager that 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 Risk Mitigation Program will operate** within your organization. As part of rule and policy development, the Insider Risk Program should also identify practices for safeguarding sensitive personnel information along with consequences for violations of internal rules committed by Insider Risk Program team members. Insider Risk 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 Risk Mitigation Program Plan is included in the **Resources** section.

- You should also **ensure that Insider Risk Mitigation Program personnel are properly trained** to conduct their duties. Insider Risk 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 for more information.

ESTABLISHING AN INSIDER RISK PROGRAM (Cont.)

DETECTING AND DETERRING INSIDER THREATS

- The purpose of an Insider Risk Mitigation Program is to proactively deter, detect, mitigate, and report threats associated with trusted insiders. These actions make up your daily operations. Insider Risk 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 Risk Programs 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 Risk Awareness training. You can also maintain workforce awareness of insider risks and employee reporting responsibilities year round by instituting a vigilance campaign. Insider Risk Programs can also conduct internal evaluations. These are small exercises used to test your workforce's knowledge of insider risk 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 for access to free training and awareness materials.
- **Reporting Procedures**. Your Insider Risk Program must establish reporting procedures for the general workforce. Those that witness potential indicators should know exactly when, where, and how they can report the information. Prepare procedures for "walk-ins" or those that may want to report their information face to face. Procedures should also include hotlines or dedicated email addresses. Consider providing means for anonymous reporting. Individuals should be encouraged to self-report any issues they may be experiencing. One of the goals of an Insider Risk 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 Risk 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 risk mitigation responses.
- **Organizational Justice**. As a best practice, Insider Risk 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 Risk 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.

RETURN TO MAIN PAGE

ESTABLISHING AN INSIDER RISK PROGRAM (Cont.)

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**, in order 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 retraining. Another example would be access control logs indicating an employee is working irregular hours or has unexplained absences from work. User Activity Monitoring 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.

- Now that you've established an Insider Risk Mitigation Program, it's time to employ risk management and mitigation strategies. Your Insider Risk 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 to learn more.

INSIDER RISK MANAGEMENT STRATEGY

RISK ANALYSIS

Risk based analysis allows the Insider Risk Mitigation 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 food and agriculture 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 Risk Mitigation Program is to protect the assets that are required by law and policy (such as those impacting food defense and food safety) and/or that provide your organization with a competitive advantage (such as proprietary data or processes). A **critical asset can be thought of as something of value** that which if destroyed, altered, or otherwise degraded would impact confidentiality, integrity, or availability and have a severe negative affect on the ability for the organization to support essential missions and business functions.

- **Critical assets can be both physical and logical (i.e. on computers)** and can include facilities, systems, equipment, and technology. An often-overlooked aspect of critical assets is intellectual property. This may include proprietary software and product formulas, customer data, schematics, and internal manufacturing and distribution processes. The organization must keep a close watch on where assets, including data, are 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. Note that assets may be at risk at any point in your supply chain and third party vendors and suppliers that are given access to your assets also have the potential to pose insider threats.

- 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?
  - Who has access to these assets?
  - 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 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 risks.

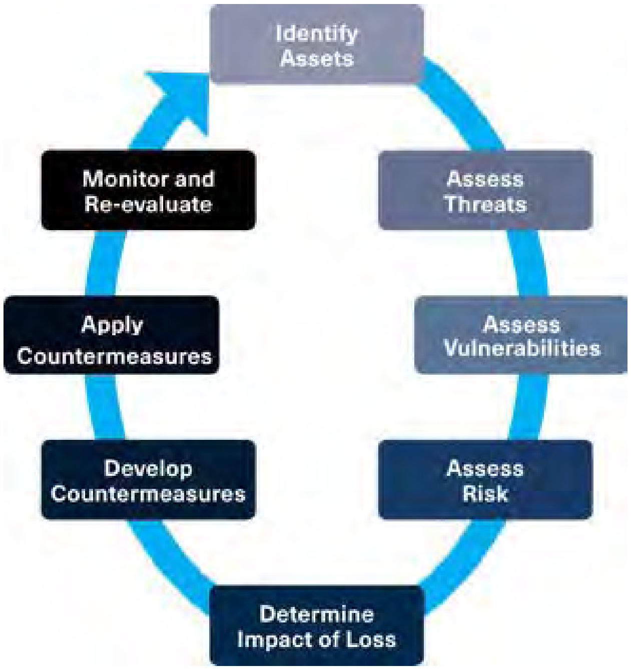
RETURN TO MAIN PAGE

INSIDER RISK MANAGEMENT STRATEGY (Cont.)

CONDUCTING A RISK ASSESSMENT

The Risk Management Process
Risk management is a 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 (consider threats in relation to identified 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 click here

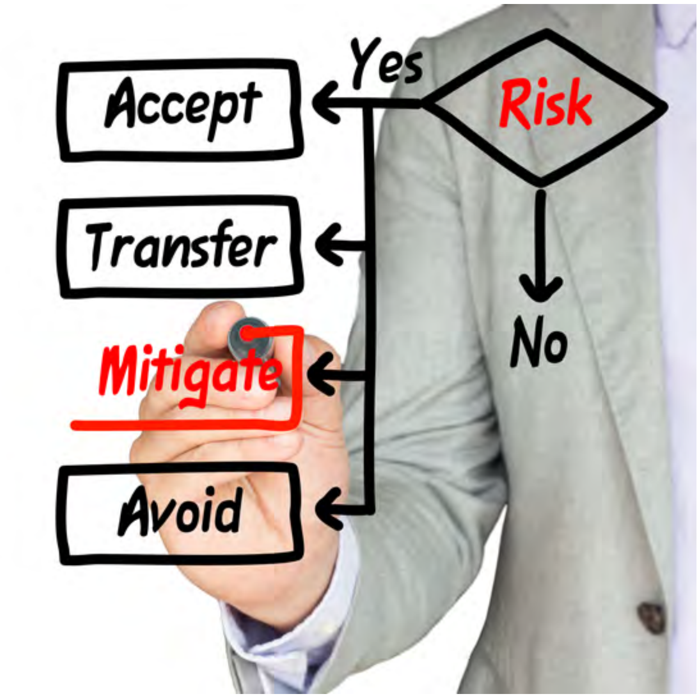
- Once you have identified critical assets, work to assess and analyze threats to, vulnerabilities of, and consequences of disruption to your organization.
- Ensure that your assessment considers the physical, cyber, and human elements of security and resilience; supply chain issues; and your interdependence on vendors, partners, and other critical infrastucture sectors.
- Translate your analysis into actionable countermeasure that can be deployed to reduce or mitigate risks and inform response and recovery actions.
- Consult the **Food and Agriculture Sector-Specific Plan** issued by the Department of Homeland Security.
- Consult the **Food Safety Modernization Act** final rule on Mitigation Strategies to Protect Food Against Intentional Adulteration issued by the Food and Drug Administration for further information on vulnerability assessments.
- You may also consider implementing the Risk Management Framework (RMF) for information systems which can help mitigate risks from cyber attack. More information on RMF is available from the **National Institute of Standards and Technology**. You can also access free training on the topic **here**.

INSIDER RISK MANAGEMENT STRATEGY (Cont.)

RISK MITIGATION

- To be effective, Insider Risk Mitigation 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, retain valuable employees, and offers intervention to help alleviate the individual's stressors.

- Your Insider Risk Mitigation 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 Risk Mitigation Program team members can assist with counseling referrals or prescribed human resource interventions which 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 Risk Mitigation Program team members from the various security disciplines, whether cyber, 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 counterterrorism 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.

INSIDER RISK RESOURCES

Insider Risk Mitigation Program Resources

FOOD DEFENSE AND BEYOND:
IDENTIFYING & RESPONDING TO
INSIDER THREATS
Everyone struggles sometimes...
Vigilance
Report to your INSIDER THREAT PROGRAM and ensure he gets the help he needs.
Food and Agriculture Sector-Specific Plan
2015
FDA Food and Drug Administration
USDA
Homeland Security
National INSIDER THREAT Task Force
2017
INSIDER THREAT GUIDE
A COMPENDIUM OF BEST PRACTICES TO ACCOMPANY THE NATIONAL INSIDER THREAT MINIMUM STANDARDS

- **Training for Insider Risk Programs**
  - CDSE
  - DHS
  - Insider Threat Awareness Materials
  - Case Studies
  - Policies and Best Practices

- **Other Federal Resources**
  - Department of Homeland Security—DHS
  - US Department of Agriculture
  - FBI
  - NCSC
  - US Food and Drug Administration
  - National Insider Threat Task Force

- **Food Defense Resources***
  - Food Safety Tech
  - Food Defense Resource Center

- **Inclusion of Resources or References does not imply endorsement by NCSC or DCSA of the opinions contained therein.**

Insider Threat Sentry Mobile Application available on Apple App Store or Google Play

SEPTEMBER 2019 | INSIDER THREAT AWARENESS MONTH

Most insider threats display concerning behaviors prior to engaging in negative events.

IF YOU SEE SOMETHING, SAY SOMETHING!

INSIDER RISK CASE STUDIES

CASE STUDIES— ACTIVE SHOOTER INCIDENTS AT FOOD MANUFACTURING FACILITIES

- Six employees were killed at an agriculture processing facility in Kansas City in July, 2004 when an employee opened fire shortly after a staff meeting. Five workers died at the scene, including the shooter, while a sixth worker died the next day. Police described the shooter as a "disgruntled employee." Coworkers told police the shooter had been laid off for several months before being called back approximately six weeks before the shooting.

- A worker at a food-service container plant near Atlanta was shot and killed in December, 2019. The suspect, a 17 year old, was a temporary employee at the company. He initially fled the area but was later arrested at a Greyhound bus station in Birmingham, Alabama and was charged with murder. He was sentenced to 13.5 years combined prison and extended supervision on September 12, 2020.

CASE STUDIES— INSIDER FOOD ADULTERATION INCIDENTS

- A supermarket in Grand Rapids, Michigan, recalled 1,700 pounds of ground beef after 111 people fell ill with nicotine poisoning. An employee at the store had mixed insecticide into the meat in an attempt to get his supervisor into trouble. Fortunately, although the amount of insecticide in the tainted meat could have been lethal, nobody died or suffered long-term health effects. The offender was sentenced to nine years in prison.

- In June 2016, a Minnesota company discovered sand and black soil in its chicken products. Video recordings were used to identify an employee as a person of interest in the case, and law enforcement was able to get a confession. She was sentenced to 90 days in jail after being convicted of two felony counts of causing damage to property in the first degree. She was also required to pay $200,000 in restitution.

CASE STUDIES— INTELLECTUAL PROPERTY THEFT IN THE FOOD AND AGRICULTURE SECTOR

- In 2014, chemical engineer Walter Liew was charged with secretly conspiring to steal technology related to proprietary manufacturing processes for titanium dioxide - the product used to achieve the brilliant white in cookie cream, automotive paint, and numerous other applications. Over the course of 14 years Liew and two co-conspirators, also insiders, stole the technology for the benefit of Chinese chemical manufacturers. Liew was convicted and sentenced to 15 years for economic espionage, possession of trade secrets, and tax fraud. One co-conspirator got two and a half years for conspiring to sell trade secrets and Liew's wife, Christina, got probation for evidence tampering.

- In 2014, six Chinese nationals were arrested for attempting to steal genetically modified corn seeds from two experimental farms in Iowa. They were employed by Chinese conglomerate DBN and its corn seed subsidiary. One of the six was the wife of the founder of DBN, and a second, Mo Hailong aka Robert Mo, was her brother who co-opted insiders from the American companies to obtain the precise geo-location of the corn seed. The US companies said they had spent billions of dollars developing the advanced corn seed. In 2016, Mo Hailong was sentenced to 36 months in federal prison for conspiracy to steal trade secrets.

Access more Insider Risk case studies.

INSIDER RISK MITIGATION PROGRAM QUICK START GUIDE

ESTABLISH your insider risk mitigation program by working with senior leadership to evaluate the risk environment. Conduct a Risk Assessment to identify critical assets, threats to your organization, unique vulnerabilities, and appropriate countermeasures to address the insider threat. Designate a senior official or program manager. Work with senior managers from throughout your company including security, human resources, legal, quality control, facilities and operations management, and information technology representatives to craft an Insider Risk Mitigation Program Plan and establish information sharing policies and mitigation strategies.

DETER insider threat activities and manage insider risk by instituting training and awareness programs for all personnel. Ensure that principles of organizational trust, fairness, and transparency are part of your work culture and communicated to employees. Evaluate work processes and security protocols such as pre-employment vetting, principle of least privilege, separation of duties, and termination procedures to ensure that insider risk considerations are in place.

DETECT behaviors and activities indicative of potential risk by encouraging reporting to front line managers, supervisors, human resources, security and insider risk program personnel. Consider establishing designated email and/or phone lines, including anonymous reporting options. Ensure employees know what to report and to whom. Establish user activity monitoring capability on sensitive systems or those that house proprietary data.

MITIGATE potential risk by addressing insider risk indicators early – before a negative event occurs. Coordinate with your multidisciplinary insider risk team to deploy proactive interventions. Many risks can be mitigated with increased training, updated security protocols, or human resources and employee assistance program strategies. Decide how the team will handle indicators and ensure fair, consistent application of mitigation strategies.

REFER insider threat incidents and/or potential risk indicators that cannot be resolved to appropriate local and federal law enforcement. Make sure employees know to call 911 when there is a threat of imminent danger.

MATURE your insider risk program over time by conducting self-assessments to determine the effectiveness of your deterrence, detection, and mitigation capabilities. Consider insider threat specific training for insider risk team personnel and coordinate with partners in your industry to identify best practices. Engage with federal agencies and organizations for access to resources.