National
INSIDER THREAT
Task Force

2017

INSIDER THREAT
GUIDE

A COMPENDIUM OF BEST PRACTICES TO ACCOMPANY THE NATIONAL INSIDER THREAT MINIMUM STANDARDS

THE INSIDER THREAT MISSION IS A
DYNAMIC EFFORT REQUIRING CONSTANT
EVALUATION, FRESH PERSPECTIVES, AND
UPDATED APPROACHES.

FOREWORD

In 2014, the National Insider Threat Task Force (NITTF) published its "Guide to Accompany the National Insider Threat Policy and Minimum Standards" to orient U.S. Government departments and agencies to the various concepts and requirements embedded within the national program. Of course, many things can change in a span of three years. The threat landscape continually evolves, technology shifts rapidly, and organizations change in response to various pressures. Thus, the insider threat mission is a dynamic effort requiring constant evaluation, fresh perspectives, and updated approaches.

As a result, the NITTF is releasing the *2017 Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*. This product is an update to the 2014 "Guide to Accompany the National Insider Threat Policy and Minimum Standards," but with new emphasis on alignment with the national minimum standards so that departments and agencies can fully interpret and meet all of the requirements. Furthermore, this 2017 guide contains best practices to help insider threat managers overcome common challenges and establish functional programs with fewer complications.

It is important to recognize and thank the U.S. Government insider threat community for your daily efforts and contributions as this collection of best practices would not be possible without your input. Simply stated, this is your guide. It is filled with your lessons learned and designed for you to use as a mechanism to build, maintain, and enhance your programs.

However, this product is by no means a culminating report for either the insider threat enterprise or the NITTF, as there is still a long road ahead. Ensuring that all applicable U.S. Government entities meet the programmatic minimums is just the first step. The NITTF is already examining ways to help programs become more effective in deterring, detecting, and mitigating insider threats and more efficient in conducting daily operations. Going forward, the NITTF will continue to lean on your support and collaboration.

The NITTF will continue to be a resource for you as you endeavor to diminish the insider threat to our national security.

TABLE OF CONTENTS

DEPARTMENTS AND AGENCIES WITH MATURE, PROACTIVE INSIDER THREAT PROGRAMS ARE BETTER POSTURED TO DETER, DETECT, AND MITIGATE INSIDER THREATS BEFORE THEY REACH A CRITICAL POINT AND POTENTIALLY HARM NATIONAL SECURITY.

INTRODUCTION

More than five years have passed since Executive Order (E.O.) 13587 required executive branch departments and agencies (D/As) with access to classified information to implement an insider threat detection and prevention program. Since then, the executive branch has made considerable progress in meeting that goal. The White House Memorandum on *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (hereinafter "*Policy & Standards*") laid out the twenty-six minimum standards that D/As are required to meet. The intent of this guide is to assist D/As in their implementation of these minimum standards.

E.O.13587 also established the National Insider Threat Task Force (NITTF) to assist in the development of an Executive Branch-wide national insider threat program. In addition to developing the *Policy & Standards*, the NITTF has become central to the continued maturation of the national insider threat community. The NITTF provides individualized technical and programmatic assistance to D/As, conducts training, disseminates best practices, and is championing the push to professionalize and standardize the insider threat career field. Perhaps most importantly, the NITTF is conducting independent assessments of D/A insider threat programs to gauge their implementation of the minimum standards. The knowledge gained from these assessments and community outreach efforts has informed much of this guide.

Program requirements contained in E.O.13587 and the *Policy & Standards* extend beyond the safeguarding of classified information on computer networks and systems. By the definition contained in the *Policy & Standards*, insider threat detection requires the establishment of capabilities that apply to classified information in all its forms, including information stored digitally as well as the activities of persons who maintain physical access to that information. For that reason, an agency program shall encompass the deterrence, detection, and mitigation of classified information residing outside the network environment.

While E.O.13587 focuses primarily on the safeguarding and sharing of classified national security information, the NITTF recognizes that many agencies possess information they consider extremely sensitive and critical even though it may not classified. While the principles and practices discussed herein are written to help agencies comply with the *Policy & Standards*, such efforts can be applied to protect a sensitive unclassified environment. In addition to E.O.13587, D/As should consult any unique authorities (statutory or otherwise) that provide the ability to expand the scope or responsibility of insider threat programs consistent with mission needs.

While every D/A with access to classified information must adhere to the requirements set forth in the *Policy & Standards*, the NITTF realizes that this effort cannot have a "one size fits all" approach. D/As are provided a great deal of latitude to develop a program tailored to their unique mission, organization, culture, and threat landscape provided they meet the twenty-six minimum standards. Because there is such departmental diversity across the United Stated Government (USG), no two programs will be exactly alike. Thus, not every lesson learned or best practice contained in this guide may be directly applicable to every D/A program. However, the NITTF hopes that the insights within this compendium offer D/As innovative and valuable ways to address challenges, enhance capabilities, ultimately comply with all programmatic requirements, and even go above and beyond the minimum standards when appropriate.

Please visit NITTF's unclassified website at **https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf#content** for additional material including policy templates, training aids, reference documents, etc.

If your D/A has any questions regarding this guide or needs assistance with program implementation, please contact the NITTF via e-mail at **NITTF-Assistance@dni.gov**.

HOW TO USE THIS GUIDE

This guide provides direction to D/As implementing the basic building blocks of an insider threat program. It begins with the sections "Helpful References" and "Laying the Foundations" which provide useful tips for D/As building programs from scratch. The next six sections of this guide track the major categories of the minimum standards: Designation of a Senior Official(s); Program Personnel; Access to Information; Employee Training and Awareness; Monitoring User Activity on Networks; and Information Integration, Analysis, and Response.

Note that the order of the six categories in this guide does not match the sequence in the *Policy & Standards* nor does it perfectly align with the process used during NITTF assessments. While these standards do not have to be implemented sequentially, they are arranged in this guide based on the logical flows of program design and activity. Essentially, the first five categories set programmatic conditions and establish information sources that ultimately enable the analysis of behavioral anomalies and appropriate resolution of insider threat issues.

Each section will follow a common format to define the major category/minimum standard, to explain in detail how to meet that standard as assessed by NITTF, and finally to present best practices for implementation.

> I. Category
>> 1. Minimum Standard
>>> • Meeting the Standard
>>> • Best Practices

This guide attempts to answer common programmatic questions posed by D/As as they strive to comply with the minimum standards. The insights contained within this document are a result of NITTF's continuous training and assistance discussions with the USG insider threat community as well as experience in assessing the progress of more than 85 D/As implementing the minimum standards. This guide supersedes the previous insider threat program guides issued by the NITTF and NCSC including the NITTF's 2014 "Guide to Accompany the National Insider Threat Policy and Minimum Standards" and the 2011 "US Government Insider Threat Detection Guide."

Please visit NITTF's unclassified website at https://www.dni.gov/index/php/ncsc-how-we-work/ncsc-nittf for additional material including policy templates, training aids, reference documents, etc. If your D/A has any questions regarding this guide or needs assistance with program implementation, please contact the NITTF via e-mail at NITTF-Assistance@dni.gov.

HELPFUL REFERENCES

1. The basic requirements for insider threat programs are contained in **E.O. 13587**, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; White House Memorandum on *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, 21 November 2012; and White House Memorandum on *Compliance with President's Insider Threat Policy*, 19 July 2013.

2. An agency must understand its personnel security responsibilities and authorities, particularly those involving clearances and classified information. To gain a better understanding of the basic requirements that govern an individual's access to classified material—including access by the government to personal information—refer to **E.O. 12968**, *Access to Classified Information*, and to **E.O. 13467**, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, as amended. Note that Section 3 of **E.O. 13764**, amends the handling and use requirements of **E.O. 13467** to allow recipient D/As to receive reports, information, and other investigative materials developed by investigative D/As during the personnel security vetting process, and those recipient D/As can use those materials for insider threat program purposes.

3. D/A insider threat programs should be knowledgeable about continuous evaluation requirements and data sources. Pursuant to **E.O. 12968**, *Access to Classified Information*, as amended by E.O. 13467 in 2008, the DNI is responsible for determining and establishing standards for continuous evaluation across the executive branch.

4. The minimum standards require the incorporation of Information Assurance (IA) information into an insider threat program. IA includes data from audit and monitoring efforts often required by other federal authority. Several federal bodies dictate information assurance practices across the government. The Committee for National Security Systems (CNSS) provides instructions and sets standards for networks and IT devices that contain, or access national security information. **CNSS Instruction 4009, National Information Assurance Glossary** provides useful IT definitions. **CNSSI 1015, Enterprise Audit Management Instruction for National Security Systems (NSS)** identifies user-attributable enterprise audit (audit logs) that can support insider threat program efforts. **CNSS Directive 504, Directive on Protecting National Security Systems (NSS) for Insider Threat, Appendix B**, defines and requires User Activity Monitoring (UAM) on all national security systems (all classified systems AND unclassified systems that contain information related to weapons systems and/or military operations). In addition to IC and CNSS requirements, the National Institute of Standards and Technology (NIST) sets national-level IT security policy for the federal government's unclassified networks. **NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**, lists hundreds of IA "control" (action items) that may be required, depending on the risk level of the networks. **NIST 800-53**, Appendix G includes a mapping of those controls to insider threat program efforts under E.O. 13587, and recommends utilizing the same insider threat practices used to protect classified information to protect controlled unclassified information (CUI).

5. The process for classifying and declassifying information, along with agency responsibilities within those processes, are covered in **E.O. 13526**, *Classified National Security Information*. Similar information pertaining to classified nuclear information can be found in the *Atomic Energy Act of 1954*. Some agencies have expanded the scope of their programs to include unclassified information, specifically CUI. These agencies should be familiar with **E.O. 13556, Controlled Unclassified Information** which establishes the program for managing CUI in the executive branch. **32 CFR Part 2002 Controlled Unclassified Information** establishes policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, to include self-inspection and oversight requirements.

6. The guidelines that address classified information requirements pertaining to the agency contractor workforce are discussed in **E.O. 12829**, *National Industrial Security Program*, 6 January 1993. *DoD 5220.22-M National Industrial Security Operating Manual, Incorporating Change 2*, 18 May 2016, requires contractors to establish and maintain insider threat programs consistent with *E.O. 13587* and the *National Insider Threat Policy and Minimum Standards*.

7. The NITTF published *Protect Your Organization from the Inside Out: Government Best Practices* in 2016. This document draws from NITTF's interaction with D/As to provide advice intended for organizations of all sizes to help them take the first steps to protect what matters most to their vital interests. This document is available on NITTF's unclassified webpage.

LAYING THE FOUNDATIONS

A   FORM A WORKING GROUP OF INTERESTED STAKEHOLDERS

B   OBTAIN VISIBLE SUPPORT FROM THE D/A HEAD

C   EMPHASIZE TO THE WORKFORCE INSIDER THREAT PROGRAM SUPPORT FOR THE PROTECTION OF PRIVACY AND CIVIL LIBERTIES

D   EVALUATE YOUR D/A'S UNIQUE ASSETS

E   EVALUATE YOUR AGENCY'S CRITICAL ASSETS

While the majority of this guide deals with the implementation of the minimum standards, this first section covers foundational best practices that are common among many mature insider threat programs.

A. Form a Working Group of Interested Stakeholders:

D/As that have not made significant progress in building insider threat programs should assemble a cross-agency working group that will meet regularly to develop the program and implement the *Policy & Standards*. The senior official should consider providing in-person periodic updates to the agency head and leadership on the group's progress. This interaction reinforces senior leadership awareness of and support for the program. Additionally, the working group can also help to develop relationships between components/offices, leading to better information sharing and cooperation. This also minimizes the possibility of unwanted surprises from program development efforts and should provide early notice to the leadership team of the need to restructure current funding allocations to support the new program.

The working group should consist of representatives from all stakeholder offices within the agency. A "stakeholder," in this context, is an agency office whose business activities place them in a position to receive and retain information pertinent to the background, conduct, and activities of agency employees. Stakeholders should include representatives from:

- • Security
- • Counterintelligence (CI)
- • Information Assurance (IA)
- • Office of the Chief Information Officer (CIO)
- • Office of the Inspector General (OIG)
- • Office of Professional Responsibility (OPR)
- • Law Enforcement (LE)
- • Human Resources (HR)

The Office of the General Counsel (OGC) or appropriate legal entity should be included as a working group member to help sort through questions that may arise about authorities and legal impediments. Civil liberties, privacy office(s), and whistleblower protection officials should also be represented. As the D/A develops a program that provides a more in-depth look into the professional and personal activities of agency employees, legal advice and participation at every stage of the working group effort will be essential.

The broad membership of the working group should guarantee wide input from across the D/A, which helps senior staff become familiar with the *Policy & Standards*.

The *Policy & Standards* address D/A actions that should apply to all cleared employees. The definitions of "employee" and "cleared employee" contained in the *Policy & Standards*, respectively, include contract personnel. With the advice of counsel, agency efforts to establish a program should include measures to incorporate the requirements of the *Policy & Standards* into the provisions of the agency's commercial contracts that involve classified information and access by contract personnel to that information. The National Industrial Security Program Operating Manual (NISPOM) governs access to classified information by contract personnel and lays out the requirements for the cleared contract workforce.

When considering the contractor environment, there is a unique three-cornered relationship that should be taken into account: the agency, its cleared contractors, and the Cognizant Security Agency (CSA). CSAs are established under E.O. 12829, and have exclusive authority within the executive branch to establish industrial security programs. Every D/A that desires to employ cleared contractors must affiliate with one or more CSAs and must follow industrial security program requirements established by its respective CSA(s). Four entities are established in E.O. 12829 as CSAs: DoD, Department of Energy, the Nuclear Regulatory Commission, and the Director of National Intelligence (DNI). Every D/A that employs cleared contractors has responsibilities to one or more CSAs. CSAs, in turn, are expected to develop and implement their industrial security programs according to the guidance found in the NISPOM. All D/As with cleared contractors must follow the security programs established by their respective CSAs.

COGNIZANT SECURITY AGENCY DISCUSSION POINTS

As the D/A insider threat working group reviews the various requirements and guidance that applies, the working group, with OGC participation, should take care to initiate a dialogue with their CSAs to ensure that, at the appropriate time, the *Policy & Standards* are applied to the cleared contractor workforce. Among the points that the working group may wish to clarify in discussion with its respective CSAs are the following:

- How will insider threat awareness training best be accomplished and documented for the agency workforce?
- How will user activity monitoring be accomplished for cleared contractors? This discussion may also require contact with service providers from other organizations when those organizations operate classified computer systems and networks that the agency uses?
- What relationship will exist between the agency program and the insider threat programs established by the various cleared contracting firms that work for the agency?
- How will the senior official responsible for insider threat mitigations at contracting firms interface with the agency's program?
- What will be the relationship between the agency program and the CSA program? How will the information integration and analysis function required by the *Policy & Standards* be accomplished for cleared contractors?
- How will the CSA, agency, and contractor firms collaborate to respond to and resolve insider threat concerns and issues?
- How will the access to information requirements of the *Policy & Standards* apply to information held by the contracting firm?
- Are there records retention issues to consider when the records contain contractor information?

The working group and the senior official should present the D/A program draft implementation plan and a draft insider threat policy to the agency head for approval as soon as possible. The approval should include resource allocations sufficient to immediately establish a program office to execute the new insider threat policy and the program implementation plan. Should resources not be immediately available to implement all the minimum standards, agencies should use a risk assessment to determine which standards will be funded. Acceptance of risk should be identified in the implementation plan and briefed to and approved by senior agency leadership.

Once the policy and implementation plan are approved, the working group should establish a program office—with a program manager and personnel dedicated to implement the policy. With the establishment of the program office, it may be possible for the insider threat working group to meet less frequently and transfer all or most of its responsibilities to the new program office. As the program office is being assembled, it should be introduced to the entire D/A workforce, preferably by senior leadership, as part of the "rollout" of the D/A's new policy and implementation plan. This roll-out can serve to introduce the new policy, as well as act as an initial training activity by the D/A, which will help meet the requirements of the training and awareness minimum standard.

B. Obtain Visible Support from the D/A Head:

The minimum standards list several responsibilities that must be accomplished by the D/A head. In addition to those basic responsibilities, successful insider threat programs receive strong, personal, and visible support from the agency head. Leadership endorsement of the program is greatly enhanced when D/A leadership lend their name and/or image to workforce communications about the program. This is especially important in D/As outside the IC and DoD. Employees in these agencies may not have strong security awareness and may be hesitant at first to support insider threat programs. Agency heads who are visibly involved in program awareness provide a valuable level of emphasis to the workforce and drive positive change towards a supportive organizational culture.

The D/A head may already have various internal communications methods to inform the workforce of the importance of the insider threat risks. "All Hands" meetings, community forums, newsletters, and blogs, for example, may already be employed and can be effective communication vehicles through which D/A leadership can frame and emphasize the insider threat mission.

C. Emphasize to the Workforce Insider Threat Program Support for the Protection of Privacy and Civil Liberties:

Insider threat programs involve the integration of personal data. Highlighting the protection of employee privacy rights and civil liberties is essential in securing workforce support for insider threat programs. Insider threat programs and agency leadership should socialize this program to the workforce and should be as transparent as operationally possible. Employee support of the program is essential and the workforce must see the program as fair and respectful of employee reputations. There are numerous points of emphasis:

- Privacy protections and oversight obligations are prevalent throughout the *Policy & Standards*;
- Insider threat programs are designed to monitor and detect anomalous behavior, not to monitor people. Insider threat programs do not target individuals;
- Systems of Record Notices (SORNs) should be in place to comply with the requirements of the Privacy Act;

• Data sources, triggers, etc. need to be rationally related to insider threat. Insider threat program focus should not be overly broad; it should be tailored to the approved scope of the program;

• Personnel conducting analysis should be trained in unconscious bias to aid their contextualization of events;

• Numerous legal forums have brought together legal counsel and privacy officials from across the community to discuss insider threat program specifics.

D. Evaluate Your D/A's Unique Authorities:

The working group should identify policies and procedures already in place that may have an impact on the establishment of the program. The working group should then consider how current agency policy and the current agency environment may require modification in order to comply with the *Policy & Standards*. These discussions of the D/A's particular environment will help tailor its program to meet the distinct needs, mission, and systems of the D/A.

There is no single "solution" defining where the program should reside within an agency. The program may be independent, reporting through the designated senior official to the D/A head. It can be situated within the security office, because it may already be the focal point to resolve incidents involving the unauthorized disclosure of classified information. Alternatively, it may be situated within a separate counterintelligence office, which normally is focal point for handling incidents of suspected espionage. Wherever the program resides within the organizational structure, it should develop and maintain close collaborative ties with the D/A:

  • Director of Security,
  • Director of Counterintelligence
  • Chief Information Officer
  • Inspector General
  • General Counsel
  • Human Capital Resource Officer
  • Civil liberties, Whistleblower and Privacy Officials
  • Chief Financial Officer

E. Evaluate Your Agency's Critical Assets:

E.O.13587 and the *Policy & Standards* are focused on safeguarding classified information and networks. The working group should determine whether the agency has identified its other critical assets—those elements of the agency's mission that are essential to the agency and to national security and which, if damaged, stolen, or otherwise exploited, would have a damaging effect on the agency, its mission, and national security.

Although the program will apply to cleared personnel, the working group should consider whether it wishes to apply its program to other agency critical assets that are sensitive but unclassified.

The agency should have a process in place for determining its critical assets and assessing its risk posture as a cornerstone of an effective program. If the agency has not identified its critical assets, then it should immediately begin the effort to do so and to assess the risks to those assets, parallel to the effort to establish the program. The establishment of an insider threat working group provides an opportunity to review, across the agency, the maturity of its critical asset risk assessment process.
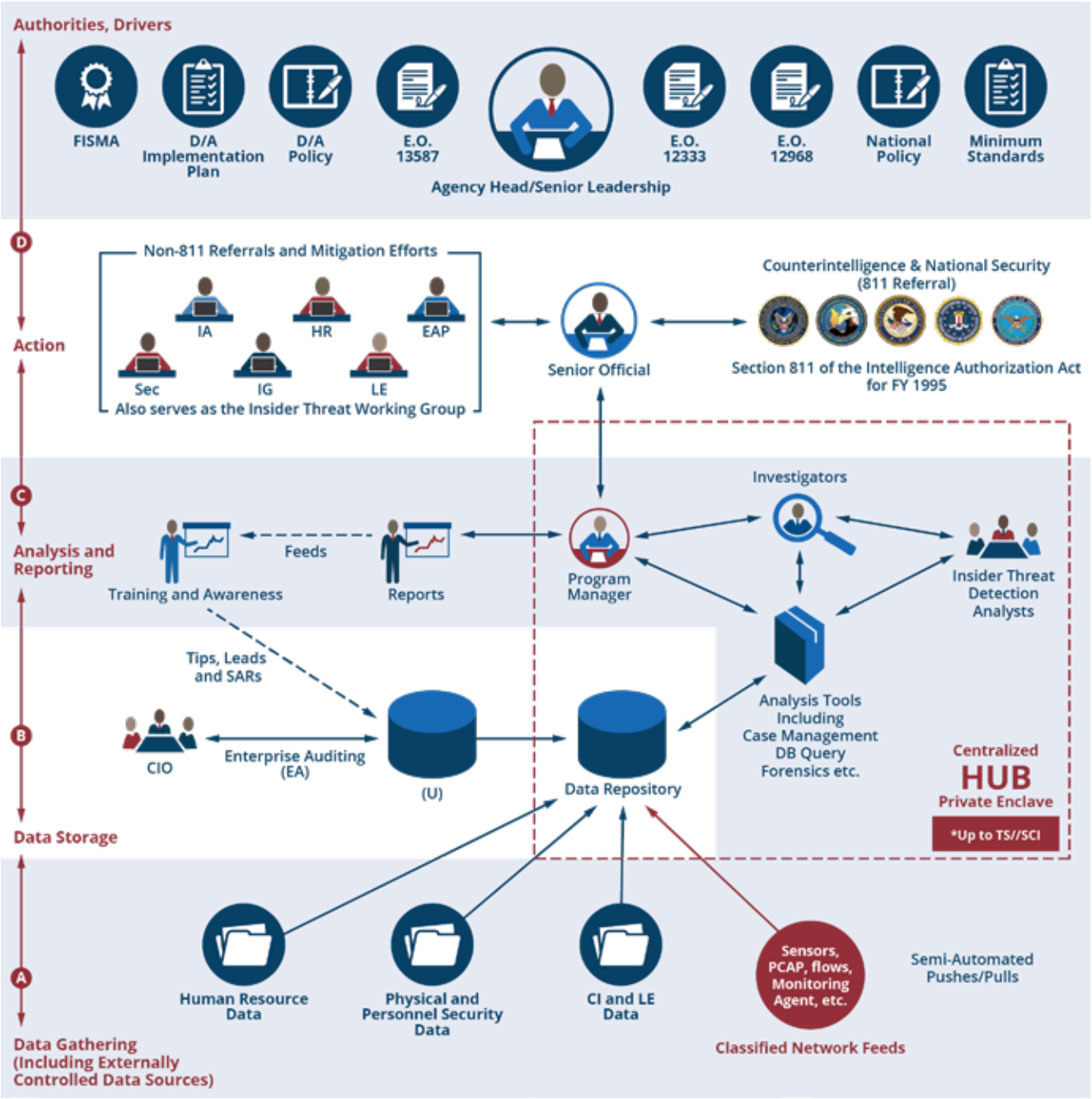
I. DESIGNATION OF SENIOR OFFICIAL(S)

1. SENIOR OFFICIALS SHALL PROVIDE MANAGEMENT AND OVERSIGHT OF INSIDER THREAT PROGRAM AND PROVIDE RESOURCE RECOMMENDATIONS TO AGENCY HEAD.

2. SENIOR OFFICIALS SHALL DEVELOP AGENCY INSIDER THREAT POLICY, APPROVED BY AGENCY HEAD WITHIN 180 DAYS OF EFFECTIVE DATE OF NATIONAL INSIDER THREAT POLICY.

3. SENIOR OFFICIALS SHALL SUBMIT A PLAN FOR ESTABLISHING AN INSIDER THREAT PROGRAM AND REPORTING PROGRESS WITHIN THAT AGENCY.

4. SENIOR OFFICIALS SHALL ENSURE AGENCY'S PROGRAM IS DEVELOPED AND IMPLEMENTED IN CONSULTATION WITH THAT AGENCY'S OFFICE OF GENERAL COUNSEL AND IN ACCORDANCE WITH LAWS.

5. SENIOR OFFICIALS SHALL ESTABLISH OVERSIGHT MECHANISMS TO ENSURE PROPER HANDLING OF RECORDS AND DATA, ENSURING ACCESS TO DATA IS RESTRICTED.

6. SENIOR OFFICIALS SHALL ENSURE ESTABLISHMENT OF PROCEDURES FOR RETENTION OF RECORDS AND DOCUMENTS NECESSARY TO COMPLETE ASSESSMENTS.

7. SENIOR OFFICIALS SHALL FACILITATE OVERSIGHT REVIEWS BY OFFICIALS DESIGNATED BY AGENCY HEAD TO ENSURE COMPLIANCE WITH INSIDER THREAT POLICY GUIDELINES.

Each agency head shall designate a senior official or officials, who shall be principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resources (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat. Senior Official(s) shall:

The first category of minimum standards creates the foundation for a successful insider threat program. These standards ensure that programs have access to and inform agency heads, have policies and procedures that are effective and legal, and are developed and overseen by independent entities. These standards are therefore crucial to ensure that programs have solid legal, policy, and privacy underpinnings.

1. *Provide management and oversight of the insider threat program and provide resource recommendations to the agency head.*

Meeting the Standard:

D/As solidify agency support for their insider threat program by designating an official of sufficient seniority within the agency to take responsibility for development and operation of the program and to have influence in the prioritization of agency resources. Agency heads designate in writing one or more senior official(s) as responsible for the management, accountability, and oversight of the program. The senior official has direct access to the agency head for matters of insider threat concern and can exert influence up to D/A leadership, across the D/A's directorates, and down to the insider threat program. The senior official is high-ranking enough to communicate as a peer with D/A data-holders, enabling the insider threat program to negotiate with the components for information.

Best Practices:

- *Singular Accountability* – The majority of D/As designate only one senior official to manage and oversee the program.

- *Multiple Officials* – Designation of more than one senior official can be a viable option in situations where insider threat detection and prevention requires dividing responsibility among several officials (for example, where a D/A has multiple components or elements subordinate to it and/or distributed over many geographically separated facilities). In such cases, D/As establish a coordination process so that the program speaks with only one voice.

- *Primary Facilitator* – In most D/As, the senior official facilitates the integration effort, acting as the primary interface between senior leaders across the D/A to explain program requirements and elicit continuing collaboration from the offices led by those senior leaders.

- *Primary Negotiator* – In some situations, access to a particularly sensitive information source needs to be negotiated by the senior official.

- *Primary Resource Advocate* – In larger programs, the senior official(s) is the primary advocate within the D/A for program resources and overseeing program resource distribution across the entire agency. The senior official looks across all initiatives comprising the program to advocate for mission critical program requirements, and to make informed recommendations to the agency head regarding resource trade-offs.

- *Policy* – The senior official is the primary advocate to ensure all D/A policies and procedures not only comply with, but also promote insider threat program efforts.
- *Visible Symbol* – The senior official and the agency head are frequent and vocal advocates of the program through workforce messaging.
- *Natural Fit* – In a number of agencies with mature programs, the responsibility for the program is vested in a senior executive who is also responsible for the agency's security and/or CI activities. Though not required, this does seem to be a natural fit, since many of the capabilities that will be important to the program may already be resident within the CI or security structures.
- *Performance Plans* – To ensure that senior official efforts and achievements toward the mission are recognized, such responsibility should be reflected in the senior official's performance plan.

CHECKLIST

SENIOR OFFICIAL CHECKLIST

- Establish a central program office to collect and analyze information from all sources to identify insider threat concerns and to initiate appropriate response actions.
- Establish procedures by which information from across the agency will be accessible by program personnel.
- Establish processes to centrally manage all agency insider threat response actions.
- Establish response protocols and procedures.
- Disseminate across the D/A information about insider threat activities that should be shared with the program along with reporting mechanisms.
- Employ an insider threat risk assessment capability for the D/A, and incorporate the results into the organization's critical asset identification and risk assessments processes.
- Develop insider threat awareness training for the workforce per the *Policy & Standards*.

- Develop a collaborative arrangement whereby advice of counsel is regularly provided to the senior responsible official and the program office to ensure that insider threat activities stay within legal boundaries.
- Establish appropriate mechanisms to ensure the proper use of information and the adherence to privacy, civil liberties and whistleblower protections within all insider threat activities in concert with the agency General Counsel and civil liberties and privacy officials. Leverage information-gathering, analytic, investigative, and operational resources from across the D/A to ensure that each insider threat concern is documented, promptly investigated, and resolved.
- Establish a system of records, as required by the NARA, to properly record and document program activities.
- Establish a system to obtain current USG reporting on insider threats, trends, and methods.
- Conduct periodic self-assessments of the adequacy of D/A insider threat posture and compliance with E.O. 13587 and the *Policy & Standards*. The objective should be to conduct periodic reviews of the agency program using expertise external to the program. Facilitate external independent assessments (by NITTF and others) of program adequacy.
- Draft an annual report for the agency head on the progress and/or status of program.
- Develop mechanisms to regularly discuss insider threat issues with the same stakeholders that assisted in the development of the D/A's policy and implementation plan.
- Assist the D/A mission by contributing insider threat perspectives to decision makers.
- Identify resources necessary to operate an effective and comprehensive program.
- Regularly collaborate with D/A leaders as the agency head's primary advocate for insider threat preparedness. Key among these relationships will be the partnerships forged with the agency Chief Financial Officer or Chief Financial Executive to identify and justify future personnel and budgetary requirements for the program.
- Act as the D/A focal point to coordinate and respond to requests for information.
- Encourage innovation, creativity, and efficiency in solving insider threat problems.
- Build and maintain necessary internal and external partnerships to draw in expertise and collaboration from other sources. In particular, the FBI can provide invaluable insights to help a D/A determine if an insider threat concern warrants referral to the FBI for investigation. In addition, D/As that have mature programs in place will also be good sources of information and advice.
- Ensure insider threat program interests are incorporated into the organizational enterprise and considered in policy and acquisition strategies.
- Serve as an ambassador for the program while promoting a positive culture of awareness.

2. *Develop and promulgate a comprehensive agency insider threat policy to be approved by the agency head within 180 days of the effective date of the National Insider Threat Policy. Agency policies shall include internal guidelines and procedures for the implementation of the standards contained herein.*

Meeting the Standard:

D/As formalize their respective insider threat efforts in official policy via comprehensive, internal documentation to establish the program, guide operations, and set the conditions for compliance with the minimum standards. This insider threat policy can be a stand-alone document or incorporated into a larger policy document as long as it is signed by the agency head or the designated authorizing entity.

Best Practices:

- *Programmatic Tasks* – A number of D/As have composed very detailed policies achieving the following programmatic tasks that support other *Policy & Standards* requirements:
  - Establish the program and direct functional or office managers to provide support and access to appropriate data.
  - Describe the purpose of the program (detecting, deterring, mitigating insider threats) in the context of the specific D/A's mission.
  - Designate that a senior official(s) will be responsible for oversight and management of the D/A's program.
  - State which D/A employees are subject to the insider threat program (staff, contractors, detailees, military members, etc.)
  - Establish a program office, possibly including a centralized analysis and response "hub."
  - Ensure program personnel have authorized access to insider threat-related information and data from across the agency and other agencies as appropriate.
  - Ensure legal, privacy, civil rights, civil liberties, and whistleblower protections issues are addressed.
  - Mandate insider awareness training.
  - Produce annual reports on program status.
  - Designate officials to conduct independent assessment of the program's compliance with insider threat program guidelines and policies.

- *Organizational Dispersion* – Organizations that are inherently hierarchical or regionally dispersed (departments-agencies, combatant commands-sub commands) are at greater risk of experiencing gaps in coverage. D/As should not assume that a subordinate unit or a geographically distant organization has its own insider threat program. A few such entities have drafted additional layers of policy/standard operating procedures, designated POCs, and established dedicated communication channels to mitigate these organizational risks.

- *Regular Review* – Insider threat policies are reviewed on a regular basis to ensure that the guidance maintains effectiveness and adapts to any changes to laws, policies, organizational structures, and/or IT architecture.

WHAT'S IN A NAME?

The *Policy & Standards* establishes a set of core requirements for a program to deter, detect, and mitigate insider threats. However, there is no requirement to call this entity an "Insider Threat Program."

3. *Submit to the agency head an implementation plan for establishing an insider threat program and annually thereafter a report regarding progress and/or status within that agency. At a minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.*

Meeting the Standard:

D/As complete an implementation plan in writing that will provide a detailed way forward to establish the program and a mechanism to allocate resources, both internally and within the executive branch budgeting process.

One year after the implementation plan is approved, and annually thereafter, the senior official submits in writing an annual report to the agency head. This report documents annual accomplishments, resources allocated, insider threat risks identified, recommendations and goals for program improvement, and major challenges.

Best Practices:

- *Program Planning* – D/As have used the implementation plan to set milestones and achieve the following programmatic tasks:
  - Explaining program staffing and resourcing.
  - Outlining the responsibilities for a program office.
  - Delineating how information from various agency offices will be provided to the insider threat hub.
  - Outlining the agency methodology to conduct self-assessments.
  - Deciding whether to solicit outside assistance—perhaps from the NITTF or other agencies.
  - Determining initial operating capability and full operating capability dates.
  - Formulating current and subsequent fiscal year budgets.
  - Satisfying agency reporting requirements.
- *Living Documentation* – The majority of D/As treat their implementation plans as living documents that are subject to change and edited as milestones are achieved or missed.
- *Work In-Progress* – Organizations should not delay official approval of an implementation plan in order to include important policies or standard operating procedures.
- *Temporary to Permanent* – Many organizations sunset the implementation plan after the minimum standards have been achieved, with information concerning the policies and operations of the insider threat program then included in more enduring documents.
- *Annual Reports* – D/As have delivered their annual reports in a variety of formats including lengthy documents, two-page summaries, and PowerPoint briefings.
- *Self-Assessments* – One helpful tool a few programs have used is a self-assessment regime typically conducted prior to an implementation checkpoint, publication of the annual report, or independent oversight review/assessment.

DEPARTMENT/AGENCY SELF-ASSESSMENTS

The NITTF published a Minimum Standards Self-Evaluation Guide and uses it as the basis for NITTF's independent on-site assessments of D/A insider threat programs. It can simultaneously be used by D/A programs as a valuable reference tool when conducting internal self-assessments.

4. *Ensure the agency's insider threat program is developed and implemented in consultation with that agency's Office of General Counsel and civil liberties and privacy officials so that all insider threat program activities to include training are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies.*

Meeting the Standard:

E.O.13587 and the *Policy & Standards* require that insider threat programs comply with appropriate legal and constitutional requirements while ensuring that privacy, civil liberties, and whistleblower protections are enshrined in program policies and operations. As such, D/A insider programs continuously engage and collaborate with their respective OGCs and civil liberties, privacy, and whistleblower protection officials.

Best Practices:

- *OGC Portfolios* – The majority of D/As designate members of their OGC and privacy offices to have the "insider threat portfolio"; thus, allowing these attorneys and privacy officials to develop subject matter expertise on the insider threat detection mission.
- *Program Participation* – Many D/As incorporate active counsel and privacy officers into the larger insider threat working group to ensure an appropriate level of legal review and guidance for the program. They typically review decisions and documents governing the program's scope, to include:
  - Whether the program will look at all D/A personnel or only cleared personnel.
  - Whether the program will review activity on all IT networks or only classified networks.
  - If the program will focus on protecting CUI or only classified information.
  - If the program will look to other threats to personnel such as workplace violence.

- *Day-to-Day Guidance* – In more mature programs, OGC and CLPO personnel approve the procedures that guide the day-to-day operations of insider threat programs. Because program personnel handle a significant quantity of personally identifiable information and data involving individual conduct of employees, great care is exercised to ensure that the program provides adequate personal privacy and whistleblower protections. OGC and privacy personnel also review all investigative manuals, handbooks, Standing Operating Procedures (SOPs), and training programs for insider threat program personnel.

- *Authorities* – A number of D/As find that a letter or memorandum from OGC outlining the authorities for specific insider threat program functions — such as the inquiries of insider threat conduct and user activity monitoring — facilitates cooperation.

- *IGs & Whistleblower Protection* – Some D/As have benefited from consultation with IGs and whistleblower protection ombudsmen who have expertise in both the conduct of unlawful disclosure investigations as well the promotion of whistleblowing as a lawful mission and the subsequent protection of whistleblowers as sources.

- *Intel Oversight* – D/As with intelligence responsibilities also benefit from coordination with Intelligence Oversight (IO) officials responsible for local agency regulations.

5. *Establish oversight mechanisms or procedures to ensure proper handling and use of records and data described below, and ensure that access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.*

Meeting the Standard:

Insider threat programs document oversight mechanisms and procedures to protect the integrity of the insider threat mission and employees' privacy and civil liberties. These procedures are usually included in the program's policy, the handbook, response actions, or any other authority document that regulates insider threat activities. The procedures should outline how access to insider threat records and data is limited to designated program personnel. These procedures include the following:

- – Ensuring that both hardcopy and electronic records maintained by the insider threat program are only accessible to appropriate personnel.
- – Oversight mechanisms or procedures to ensure proper handling and use of systems audit logs and related employee information.
- – Procedures to ensure the protection of particularly sensitive or protected information (e.g., medical or financial information) and to ensure that information is restricted to those trained insider threat personnel who need such information to perform their authorized functions.

- – Insider threat program personnel are trained on laws and regulations regarding the protection of insider threat records.
- – Procedures should be approved by the senior official but do not require approval by the agency head.

Best Practices:

- *Access Restrictions* – Most programs ensure that access to insider threat information is restricted to only those persons authorized by the senior official. Determining appropriate access restrictions require close coordination among senior leaders, particularly between the senior insider threat official and the leaders whose element(s) "own" information.

- *Privacy Safeguards* – When more intrusive insider threat detection measures are deemed necessary, programs employ additional safeguards to compensate in proportion to any increased risks to privacy and civil liberties. These include such safeguards as:

  - – Progressively higher standards for the acquisition, retention, and sharing of information that is more sensitive or intrusive.
  - – Increased security, access controls, and auditing of data forwarded to the hub, including application of privacy enhancing technologies.
  - – Requirements to delete protected or sensitive information that has not been affirmatively determined to relate to an insider threat after fixed periods; extensions of retention periods may be required to be justified based on particular findings and approved by more senior officials.
  - – Data standards for decision making, including consideration of requiring human review at those points in each specific business process where the potential exists for adverse impact to the individual; agencies should pay particular attention to ensure that they do not acquire, retain, or share information that relates solely to constitutionally protected activities (e.g., freedom of religion or speech).
  - – Limitations on the dissemination of protected information—including appropriate guidance on retention and use of such information.
  - – Specific non-disclosure agreements (NDAs) for insider threat program personnel.

6.

Ensure the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587.

Meeting the Standard:

The records generated in support of insider threat programs must be created, collected, retained, and disposed of in accordance with appropriate laws and guidelines set forth by your agency and the National Archives and Records Administration (NARA). To satisfy this requirement, two published and approved documents are necessary: a System of Records Notice (SORN) and appropriate records retention guidelines. The SORN is required before retaining any insider threat records containing PII while record retention guidelines dictate retention periods and destruction schedules of records.

System of Records Notice: The Privacy Act requires executive branch insider threat programs that maintain records identifiable to individual employees to publish a notice in the Federal Register detailing the existence and character of the records. Depending how the individual D/A is implementing its Insider Threat program, there already may exist an applicable SORN that needs to be amended. On the other hand, it may be necessary to develop and obtain approval for a new SORN consistent with program activities.

Records Retention: NARA published a General Records Schedule (GRS) 5.6 that includes retention and disposition instructions for insider threat records within the Executive Branch. Records of insider threat activities should be maintained according to the GRS. Insider threat programs should work with their records management office or their general counsel to clarify which pieces of information created or collected by an insider threat program constitutes a record under the new GRS. Based on the way that different insider threat programs operate, some programs might not maintain every category of record listed in the GRS. Insider threat programs have guidance in writing that explains which program activities create which type of record.

ESSENTIAL ELEMENTS

OF A SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act requires D/As that maintain records in a system of record to publish a SORN. For the purposes of the Privacy Act, a system of records is defined as *a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*. Also for the purposes of that Act, a record is defined as *any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph*.

Section (e)(4) of the Privacy Act lists the following information that must be published in a SORN:

(A) the name and location of the system;
(B) the categories of individuals on whom records are maintained in the system;
(C) the categories of records maintained in the system;
(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
(F) the title and business address of the agency official who is responsible for the system of records;
(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
(I) the categories of sources of records in the system.

RECORDS RETENTION

Currently **44 U.S.C. Chapter 31** and other existing laws and regulations require federal agencies to develop and implement records management policies and programs that:

- Identify records needed to conduct agency business.
- Create and preserve records that document the organization, functions, programs, policies, decisions, procedures, and essential transactions of the agency. This includes records necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.
- Manage records according to NARA-approved records schedules that determine where and how long records should be maintained, and transfer permanent records to NARA.
- Ensure that an agency addresses the creation, maintenance, use, and disposition of databases, e-mail, web records, digital audiovisual materials, and records created from new and emerging technologies.

Best Practices:

- *SORN Publication* – Several D/As have published SORNs in the Federal Register. Insider threat programs without a published a SORN should review the SORNs that have already been approved as they provide a starting point for D/As that are just starting to grapple with "routine use" and disclosure questions.

- *SORN Exemptions* – A number of D/As place exemptions within their SORNs allowing them to protect sensitive activities and information. Insider threat programs work closely with OGC and privacy officials to ensure they are properly exempted from certain disclosures under the Privacy Act.

- *Records Management* – Many insider threat programs maintain a close relationship with their agency records management office. As programs mature, they create new types of documents and collect new sources of information. Working closely with the records management office ensures that programs know what information constitutes a record and what does not.

7. *Facilitate oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy and civil liberty protections.*

Meeting the Standard:

D/As heads designate one or more entities to conduct oversight reviews of the insider threat program to ensure compliance with insider threat policy guidelines, legal, privacy, and civil liberty protections. These entities are notified of this responsibility and are familiar with insider threat authorities and requirements.

Best Practices:

- *Review Independence* – Oversight reviews are conducted by an organization unaffiliated with the D/A's insider threat program. This separation allows the officials conducting the review to be free from the influence of insider threat program leadership. It also helps provide an outside, unbiased interpretation of insider threat program actions untainted by "group think."

- *Review Designation* – In many organizations, officials from OGC, IG, or similar offices are designated to conduct such reviews. In those D/As that have created an insider threat working group with stakeholders from across the organization, the legal or IG representative to the insider threat working group is not involved in the oversight reviews.

- *Review Arrangements* – Some programs develop agreements with an external entity to conduct oversight reviews. This takes the form of a department reviewing the program of a subordinate entity or two peer D/As entering into a reciprocal agreement. Such arrangements promote consistency across the national insider threat enterprise and allow programs to share practices and lessons.

- *Review Documentation* – Most D/As formalize the oversight process with written documentation with records compiled documenting date of the review, the scope of the review, the identity of the reviewers, and any outcomes or recommendations generated.

II. INSIDER THREAT PROGRAM PERSONNEL

1. ENSURE PERSONNEL ARE FULLY TRAINED IN COUNTERINTELLIGENCE AND SECURITY FUNDAMENTALS.

2. ENSURE PERSONNEL ARE FULLY TRAINED IN AGENCY PROCEDURES FOR CONDUCTING INSIDER THREAT RESPONSE ACTIONS.

3. ENSURE PERSONNEL ARE FULLY TRAINED IN APPLICABLE LAWS AND REGULATIONS REGARDING THE GATHERING, INTEGRATION, RETENTION, AND SAFEGUARDING OF DATA.

4. ENSURE PERSONNEL ARE FULLY TRAINED IN APPLICABLE CIVIL LIBERTIES AND PRIVACY LAWS, REGULATIONS, AND POLICIES.

5. ENSURE PERSONNEL ARE FULLY TRAINED IN INVESTIGATIVE REFERRAL REQUIREMENTS OF SECTION 811 OF THE INTELLIGENCE AUTHORIZATION ACT FOR FY 1995.

Because insider threat programs depend on collaboration among multiple offices and the synthesis of many disparate information sources, personnel associated with these efforts need fundamental knowledge across a wide range of disciplines. Thus, a training regime is necessary to ensure that all relevant insider threat staff possess the basic levels of understanding needed to perform their duties appropriately.

This category applies to "personnel assigned to the insider threat program." Individual D/As (with insider threat programs of diverse shapes and sizes) will be responsible for determining who it considers the insider threat program personnel. This scope ranges from smaller programs with one dedicated program manager and designated working group members to large hubs with dozens of assigned officers. D/As will be responsible for ensuring that appropriate personnel receive the necessary training.

The NITTF has not levied specific requirements governing training frequency, curricula, certifications, etc. because of the diversity across departments in hub personnel composition and available training resources. Thus, a great deal of leeway has been given to D/As to manage these requirements as they deem appropriate as long as the spirit and intent of the standards are met. Below are a few best practices D/As are utilizing to help meet these requirements:

- Internal, functional representatives train fellow personnel on select matters. For example, the OGC liaison to the hub provides a briefing on applicable laws and regulations.
- Employees newly assigned to the program undergo a "boot-camp" style orientation to gain basic knowledge prior to engaging in programmatic activities.
- Training is done on a continual basis.
- Documentation of training is critical to managing staff needs and demonstrating completion during independent assessments.
- Designate one program member as a training manager to keep training records for the insider threat program personnel, regularly schedule blocks of time in which experts (in privacy, CI, records retention, etc.) provide refresher training to program personnel, and track external insider threat training opportunities.
- Training funds are budgeted to ensure resources are dedicated to completing these requirements.
- While it is important for insider threat program personnel to be familiar with all the related functions, they should strive to develop a "discipline agnostic" approach to analyzing behavioral anomalies.

Agency heads shall ensure personnel assigned to the insider threat program are fully trained in:

1. *Counterintelligence and security fundamentals to include applicable legal issues;*

Meeting the Standard:

Insider threat programs possess the counterintelligence and security expertise needed to identify potential insider threat activity while understanding the scope of their D/A authorities and the limits of their activities. D/As demonstrate they have the requisite CI and security knowledge resident within their insider threat programs either through formal training courses or assigning CI and security professionals to the program. As a result, programs view seemingly innocuous events through CI and security lenses, looking for indicators of adversarial threats or malicious activities. All program personnel know what CI and security steps are permitted under their specific authorities.

Best Practices:

- *CI/Security Training* – Most D/As recommend that all insider threat program personnel have some level of formal training in CI and security principles, techniques, and tools.

- *CI/Security Expertise* – CI and security expertise is critical within a program's integration and analysis hub to analyze information, investigate, and resolve insider threat concerns.

- *Training Options* – Some programs utilize The Defense Security Service Center for Development of Security Excellence (DSS/CDSE) for insider threat e-learning, webinars, and job aids via their website at http://www.cdse.edu/catalog/insider-threat.html.

THREAT HUB OPERATIONS

NITTF offers a three-day instructor-led Insider Threat Hub Operations Course approximately eight times a year. It is a practical, scenario-based course designed to expose insider threat personnel to realistic events in the daily operations of an insider threat program. It introduces and exercises the basic functions of an insider threat program's centrally managed "hub" capability to gather, integrate, analyze, and respond to potential insider threat information. While the NITTF Hub Operations Course, in and of itself, does not satisfy the minimum standards for insider threat personnel training, it is an effective underpinning for meeting and exceeding those training standards.

2. *Agency procedures for conducting insider threat response action(s);*

Meeting the Standard:

All insider threat program personnel know how to respond to a referral or anomaly while not violating the law or prejudicing a subsequent investigation. To fully train insider threat personnel on response actions, programs must first have their approved response actions documented in a policy or SOP (also a minimum standard). These procedures are informed by applicable D/A authorities and approved by the OGC and senior official.

Best Practices:

- *Authorities* – One agency initiated this process by answering the question: What authority does the agency have to conduct insider threat inquiries and in what agency office(s) is that authority vested? In most cases, a D/A the authority and responsibility to investigate concerns that arise with respect to the safeguarding of classified information within the D/A. The limits of that authority, however, are matters on which agency legal counsel advise.

- *Terminology* – In some D/As, a distinction is made between administrative inquiries and investigations, with the latter performed only by entities having law enforcement authority under the law. In other communities, investigations fall completely within the legal authority granted to the agency head, albeit with some stipulations that, in certain matters or under certain conditions, the role of the FBI may take precedence.

- *OGC Support* – OGCs provide program personnel with appropriate advice and guidelines to determine when information received meets criteria requiring referral of the information to other investigative agencies.

- *Investigative Designation* – Some large civilian D/As, with multiple subordinate components, likewise require that all investigative activity meeting certain parameters be conducted by a particular office or another investigative agency (such as the FBI through an 811 Referral).

- *One SME Approach* – In many cases, an individual with significant insider threat experience at that D/A provides program personnel a block of instruction on response actions.

- *Regular Exercise* – Many programs regularly exercise their procedures to capture lessons learned and update guidelines accordingly.

3. Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;

Meeting the Standard:

Insider threat program personnel know how to collect, retain, protect, and use sensitive information from diverse sources appropriately and will be aware of the consequences of intentionally or unintentionally mishandling insider threat data. Insider threat programs aggregate and analyze diverse types of sensitive records including Personally Identifiable Information (PII), thus requiring oversight mechanisms to ensure proper handling and use of insider threat records. All insider threat program personnel receive training on these laws and regulations tailored to the unique circumstances of insider threat.

Best Practices:

- *Annual Review* – D/As conduct an annual review of record laws, policies, and regulations.

- *Information Safeguarding* – Program personnel receive periodic training in the proper use, retention, and safeguarding of all insider threat information they receive.

- *Records Management* – Representatives from the records management office, general counsel, and privacy office can provide blocks of instruction to the program personnel.

- *New Employees* – Recently assigned staff are trained by shadowing an experienced member of the insider threat program and through on-the-job training.

4. Applicable civil liberties and privacy laws, regulations, and policies; and

Meeting the Standard:

Program personnel who access insider threat records know how to collect, retain, protect, and use sensitive information without violating D/A employees' privacy or civil liberties. Because insider threat programs typically access employee PII and user activity information that could be career-damaging or highly embarrassing, it is crucial that insider threat personnel receive training in applicable privacy and civil liberties rules.

Best Practices:

- *Legal Support* – Training can be conducted by representatives from the OGC or the civil liberties and privacy office representatives who advise the insider threat program.

- *Authority Limits* – One department focuses on the limits to the agency's investigative authority, the boundaries within which an agency inquiry or investigation can be conducted, and the proper collaborative relationship that exist between the agency and external law enforcement entities, such as the FBI.

- *Investigative Integrity* – Other organizations emphasize that any inquiry or investigation into an insider threat concern is conducted in a manner that will preserve the integrity of information for use as evidence in a subsequent criminal proceeding, should the need arise.

- *Continuous Consultation* – Several programs have policies that mandate consultation with agency counsel, privacy/civil liberties, and whistleblower professionals during insider threat inquiries/investigations.

- *Employee Freedoms* – Many emphasize that insider threat response activities must not be used for political purposes, obstructing first amendment rights, or retaliating against whistleblowers.

- *Documentation* – Most D/As document training status, time, and content because such verification provides an important defense if an insider threat program is accused of violating privacy or civil liberties of employees.

GARRITY WARNING

- A Garrity Warning is an advisement of rights usually administered to federal employees/contractors in internal investigations.
- Advises interviewees of their criminal and administrative liability for any statements they may make.
- Advises interviewees of their right to remain silent on any issues that tend to implicate them in a crime.
- Promulgated by U.S. Supreme Court in Garrity v. New Jersey 385 U.S. 493 (1967).
- Helps preserve the evidentiary value of statements provided by individuals during internal administrative inquiries, should the matter also result in criminal investigation.
- Typical Warning: "You are being asked to provide information as a part of an internal and/or administrative investigation. This is a voluntary interview and you do not have to answer questions if your answers would tend to implicate you in a crime. No disciplinary action will be taken against you solely for refusing to answer questions. However, the evidentiary value of your silence may be considered in administrative proceedings as part of the facts surrounding your case. Any statement you do choose to provide may be used as evidence in criminal and/or administrative proceedings."

5. *Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal entity, such as a security office or Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.*

Meeting the Standard:

Insider threat programs are knowledgeable on executive branch-wide referral requirements found in Section 811 of the FY1995 Intelligence Authorization Act as well as agency-specific referral requirements to internal and external entities. For example, personnel are aware that the FBI must be advised immediately of any information, regardless of origin, that indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power—as required by *Section 811 of the Intelligence Authorization Act for Fiscal Year 1995*. (It should be noted that the FBI has investigative tools to gather evidence that may not be available to an individual agency. These may include National Security Letters, Foreign Intelligence Surveillance Act warrants, technical collection activities, and surveillance teams.) Program personnel are also aware of requirements to refer matters to the OIG or other internal entities.

Best Practices:

• *Coordination* – Mature programs typically develop close relationships with their local FBI field office. Open channels of communication with the FBI keep insider threat programs appraised of evolving threats to government agencies and helps hubs identify behaviors and anomalies that should be referred to the FBI.

• *Requirements* – Knowledge of 811 referral requirements is acquired through past professional experience or by attending information sessions hosted by the FBI or NITTF.

• *Documentation* – Representatives from OIG and OGC can brief program personnel on specific referral requirements which should already be comprehensively detailed in policy documents.

INSIDER THREAT PROGRAMS DEPEND ON COLLABORATION AMONG MULTIPLE OFFICES AND THE SYNTHESIS OF MANY DISPARATE INFORMATION SOURCES.

III. EMPLOYEE TRAINING AND AWARENESS

1. PROVIDE INSIDER THREAT AWARENESS TRAINING TO ALL CLEARED EMPLOYEES.

2. VERIFY THAT ALL CLEARED EMPLOYEES HAVE COMPLETED THE TRAINING.

3. ESTABLISH AND PROMOTE AN INTERNAL SITE FOR ALL CLEARED EMPLOYEES PROVIDING INSIDER THREAT REFERENCE MATERIAL AND A MEANS OF ELECTRONIC REPORTING.

Agency heads shall ensure insider threat programs:

1. *Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information, and annually thereafter. Training shall address current and potential threats in the work and personal environment, and shall include, at a minimum, the following topics:*

   a. *The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials;*
   b. *Methodologies of adversaries to recruit trusted insiders and collect classified information;*
   c. *Indicators of insider threat behavior and procedures to report such behavior; and*
   d. *Counterintelligence and security reporting requirements, as applicable.*

A highly aware workforce is key to the early detection and prevention of malicious insider threat conduct. Analyses of espionage cases provide examples of employees who disclose—only after an arrest—that they had noticed suspicious conduct of a colleague. They may have kept silent because they did not consider it sufficiently important to take action, did not recognize the observed conduct as significant, did not want to be identified as a "snitch," or did not know how to report the conduct.

It is important to invest time and resources to continuously educate the workforce on the risks associated with insider threats. This includes training on how to recognize and appropriately report anomalies and indicators. Training drives home the message that vigilance is necessary because of the enormous damage that can be caused by malicious insiders. The extraordinary damage caused by mass unauthorized disclosers of classified information demonstrates the harm that can result from an undetected or unreported malicious insider. When properly trained on insider threat indicators and reporting procedures, the workforce can become a force multiplier forming, in effect, an insider threat early warning system for the agency.

Meeting the Standard:

Create a culture of insider threat awareness among the D/As cleared population so personnel understand the dangers of malicious insiders, how to identify adversarial methodologies or anomalous behaviors, and appropriate reporting requirements. All cleared agency personnel, to include contractors and assigned military members, are required to complete this training within 30 days of gaining access to classified information and annually thereafter to reinforce and refresh these messages.

Best Practices:

- *Advocacy* – Some D/As have enshrined the training requirement for cleared employees in the agency's insider threat policy signed by the agency head, which helps ensure support for insider threat training.

- *Modulation* – Awareness training is more effective if delivered in one course module that incorporates all four of the key topics enumerated above. However, the requirements can be satisfactorily met via multiple, separate training modules.

- *Sharing Material* – Many D/As share awareness information and presentation material to expedite development of training. This practice is encouraged as long as briefing aids are properly tailored to the unique environment and mission of the employees receiving the training.

- *Audience Expansion* – While the minimum standards require only cleared personnel to receive insider threat awareness training, some D/As require all agency personnel to receive this training.
In many agencies, uncleared personnel are in a position to observe behavioral changes or anomalies evident in their cleared coworkers. Universal insider threat training can also be useful to an agency trying to protect extremely sensitive unclassified information. In this case, the wider agency population will know how to report an uncleared employee with access to extremely sensitive information that is exhibiting insider threat indicators.

- *Continuous Refinement* – Several D/As periodically review and update training content.

- *Supplemental Training* – Some D/As supplement the annual training requirement by providing a series of insider threat seminars tailored for specific segments of the D/A population.

INSIDER THREAT AWARENESS COURSES

The NITTF has directed that D/As that have not developed an insider threat awareness course by September 30, 2015, will use the Defense Security Service (DSS)/Center of Security Excellence (CDSE) course entitled "Insider Threat Awareness Course." This unclassified course is available on the DSS/CDSE website and takes approximately 30 minutes to complete.

2. *Verify that all cleared employees have completed the required insider threat awareness training contained in these standards.*

Meeting the Standard:

Agencies have mechanisms in place to gather and track insider threat training statistics for the agency's cleared personnel and furnish training statistics (percentage of workforce current and compliant) upon request.

Best Practices:

- *Simple Process* – D/As with small cleared populations have met this standard using a simple spreadsheet, provided the spreadsheet is protected and backed up to prevent loss of data.

- *Systematic Process* – D/As with larger cleared populations typically use a Learning Management System (LMS) or some type of automated tracking system. This allows for the tracking of training statistics in real-time which enables the tracking of current compliance and identification of individuals who have yet to complete insider threat training.

- *Combination Tracking* – Some organizations have combined insider threat training with other required training modules (counterintelligence training, for example). When other components of an agency provide/track such training, the insider threat programs establish arrangements for acquiring updates and statistics.

- *Deficiency Follow-Up* – A functioning tracking system/procedure permits follow-up action by the senior official with those agency offices where participation appears weak, as well as permitting the program to highlight individuals who have yet to receive awareness training.

- *Participant Feedback* – Many programs solicit feedback regularly from audiences and maintain metrics to gauge the effectiveness of the training. Some measures include incident reports received by the insider threat program within a short period of training completion and recorded comments from audiences using feedback forms.

- *Access Revocation* – Some D/As link completion of insider threat awareness training with maintaining access to D/A IT systems and in some cases revoke network access if an employee is non-compliant.

3. *Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the insider threat program.*

Meeting the Standard:

D/As have an identified network location/website accessible to all cleared personnel that provides insider threat resources to the cleared workforce and provides a secure reporting channel to the insider threat program. The site must contain information on insider threat indicators and applicable reporting procedures. Additionally, it must include a secure, electronic means for reporting matters to the program while preventing access to anyone outside of the insider threat program. A reporting method that is visible to members of the counterintelligence office or law enforcement community who are not also members of the insider threat program is not considered "secure" for these purposes. The requirement that the reporting method be secure does not require it to be anonymous. Additionally, the site includes links to insider threat training courses, privacy information, and relevant D/A policies.

Best Practices:

• *Network Placement* – Although it is recommended that the insider threat site be hosted on a classified network, it can be placed on an unclassified network, or both when feasible.

• *Platforms* – Many D/As have a webpage or SharePoint site complete with drop-down menus and text boxes. The reporting link can be as simple as a link that opens up a pre-addressed email to the insider threat program.

• *Accessibility* – While the minimum standards only require that the site be accessible to cleared personnel, most D/As make it accessible by the entire workforce.

• *Advertising* – Some programs utilize their insider threat awareness campaigns to advertise the network site to make sure employees know where to go.

• *Public Relations* – It is extremely important to gain workforce buy-in through proper messaging. Some programs have engaged their public relations staff to assist in developing language and materials.

CAMPAIGNS

Some agencies have devised an ongoing insider threat awareness campaign for the workforce that goes beyond the EOD and once-a-year training requirements. These campaigns address workforce concerns about privacy and civil liberties, build workforce knowledge and support for insider threat programs, and educate the agency population on current adversarial tactics. Such campaigns incorporate posters in the workplace, displays on agency homepage that link to the insider threat program, speakers who address insider threat topics of interest to the workforce, and efforts to include insider threat awareness in other agency training or exercises.

IV. ACCESS TO INFORMATION

1. DIRECT COMPONENTS TO PROVIDE ACCESS TO INFORMATION TO INSIDER THREAT PERSONNEL IN ORDER TO IDENTIFY, ANALYZE, AND RESOLVE INSIDER THREAT MATTERS.

2. ESTABLISH PROCEDURES FOR ACCESS REQUESTS INVOLVING PARTICULARLY SENSITIVE OR PROTECTED INFORMATION.

3. ESTABLISH REPORTING GUIDELINES TO REFER RELEVANT INSIDER THREAT INFORMATION TO THE INSIDER THREAT PROGRAM.

4. ENSURE INSIDER THREAT PROGRAMS HAVE ACCESS TO AVAILABLE U.S. GOVERNMENT INTELLIGENCE REPORTING PERTAINING TO ADVERSARIAL THREATS.

Agency heads shall:

1. *Direct CI, Security, IA, HR, and other relevant organizational components to securely provide insider threat program personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following:*

Meeting the Standard:

The insider threat program has regular and timely access to data maintained by the relevant organizational components. Such guidance and instruction is documented in writing and signed by a senior agency official at a high enough level to direct offices from across the D/A. Programs must identify offices within the D/A that possess information needed for insider threat detection and mitigation. The D/A's policy and implementation plan include sufficient direction to ensure that the insider threat program has access to needed information and the authority to access that information.

a. *Counterintelligence and Security. All relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.*

CI and security files are rich sources of information for hub analysis. Many of these records (security violations, adjudicative files, facility access records, foreign travel and contacts, polygraph records, etc.) contain information that provides unparalleled context to an anomalous event. Insider threat programs are constantly looking for additional sources of CI and Security data to include in the insider threat program.

b. *Information Assurance. All relevant unclassified and classified network information generated by IA elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.*

Access to Information assurance (IA) data from both classified and unclassified information technology (IT) systems is a critical part of insider threat program efforts. Committee on National Security Systems Instruction 4009 (CNSSI 4009) defines "Information Assurance" (IA) as: *Measures that defend information and information systems by ensuring their availability, integrity, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection and reaction capabilities."*

IA is a broad category of capabilities that includes network health and wellness efforts, and the full scope of network security activities. Core among those capabilities, and most valuable to insider threat programs, is Enterprise Audit Management (EAM), defined by CNSSI 1015 as "the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring the maintenance of the capability." Enterprise Audit (EA) includes the logging and review of numerous, user-attributable events from IT systems. The Management of EA is typically a function of D/A's Chief Information Officer (CIO) and/or Chief Information Security Officer (CISO) , and it is important for insider threat programs to work closely with the CIO/CISO to leverage EA capabilities.

USER-ATTRIBUTABLE ENTERPRISE AUDIT EVENTS

Auditable events or activities:

- Authentication events (logons/logoffs)
- File and object events (create, access, delete, modify, permission/ownership modification)
- Writes/downloads to external devices/media
- Uploads from external devices/media
- User/group management (add, delete, modify access, suspend)
- Use of privileged/special rights events (security/log policy change, configuration changes)
- Admin/root-level access
- Privilege/role escalation
- Audit/log access
- System reboot, restart, shutdown
- Print to device
- Application logs
- Export of information
- Import of information

Attributable events indicating violations of system/target:

- Malicious code detection
- Unauthorized local device access
- Unauthorized executable
- Unauthorized privilege access
- After-hours privileged access
- System reboot/reset
- Disabling the audit mechanism
- Downloading to local devices
- Printing to local devices
- Uploading to local devices

– CNSSI 1015, Appendix B

Per CNSSI 1015, the collection of EA data and its analysis through EAM is required on all systems that hold National Security Information. Beyond National Security Systems, under the authority of the Federal Information Systems Management Act (FISMA), the National Institute of Standards and Technology (NIST) also requires EA capabilities across unclassified government systems. NIST Special Instruction 800-53 (NIST 800-53) establishes basic controls, including "Audit and Accountability." As a reference, NIST 800-53, Appendix G, maps the controls to insider threat program efforts.

C. *Human Resources. All relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.*

Personnel information retained by Human Resources (HR) offices is an important component of an effective program. Biographic personnel information, such as job title, supervisor, location, employment status, start date, termination date, break in work history, etc., is valuable in providing context for an individual and his/her actions. This information may resolve apparent anomalous conduct, saving time, money, and resources. It also provides the insight needed to make timely and effective decisions concerning disposition and future actions required to resolve an anomaly or mitigate potential risk.

There are laws and regulations that govern the collection, retention, and sharing of HR personnel information. An effective program in collaboration with its General Counsel, becomes conversant with these rules and establishes a healthy working partnership with HR to ensure that information is shared, used, handled, stored, and protected in accordance with those laws and regulations.

Beyond the basic biographic information available through HR, that office can provide additional information of value to the program, including job assignments, performance reviews, performance recognition (rewards & bonuses), awards, disciplinary actions, and proposed reductions in force. This information is valuable for identifying unmet employee expectations as well as providing mitigation for other negative indicators that may have arisen.

Best Practices:

- *Automation* – More mature insider threat programs strive to obtain regular, electronic access to relevant data repositories. The more automation – the better.

- *Timeliness* – Smaller insider threat programs that do not have the current resources to maintain electronic access have crafted procedures to ensure it is provided with relevant information upon request in a timely manner.

- *CIO Coordination* – Some programs have experienced substantial benefit from developing close and collaborative relationships with its CIO/CISOs. The program office will benefit by receiving valuable guidance about the current IT architecture, future plans, technical challenges and solutions. In return, the CIO can benefit by having a complete understanding of the program plans, challenges, policies, issues, and emerging threats to D/A information.

- *Enterprise Audit* – A number of programs stress the importance of having user-attributable Enterprise Audit (EA) data available to the insider threat even if it is via access to common Security Information and Event Management (SIEM) and/or Data Loss Prevention (DLP) tools. However, to reach a greater level of correlation, EA information is sometimes directly pushed into more robust analytic tools, along with the other insider threat program information feeds, to support comprehensive analysis.

- *Continuous Evaluation* – Some insider threat programs are coordinating with their Security offices to ensure they obtain access to Continuous Evaluation (CE) information and/or notifications.

- *Community Coordination* – Some programs are establishing interagency agreements to permit the exchange of insider threat data on employees who were previously employed or considered for employment by another agency.

USEFUL HUMAN RESOURCE/PERSONNEL RECORDS

- Position descriptions;
- Resumes and biographic information;
- Hiring, transfer, retirement, and termination records;
- Promotions and demotions;
- Tardiness complaints;
- Disciplinary and counseling statements;
- Performance evaluations;
- Award recommendations;
- Pay, care and benefits information, including payroll garnishments;
- Organizational training records;
- Substance abuse and mental health records;
- Outside employment records;
- Travel vouchers;
- Foreign visitor and assignee control records; and
- Equal opportunity complaints.

2. *Establish procedures for access requests by the insider threat program involving particularly sensitive or protected information, such as information held by special access, law enforcement, inspector general, or other investigative sources or programs, which may require that access be obtained upon request of the Senior Official(s).*

Meeting the Standard:

D/As establish in writing processes by which the insider threat program requests particularly sensitive records that cannot be shared or pushed in a constant, automatic fashion. It is sufficient to have language embedded within the D/A insider threat policy or formal SOP stating that the insider threat senior official will make a request for a sensitive record to the agency head (or other high-level official). The program must have procedures in place to ensure that such sensitive information is protected.

Best Practices:

- *Dispute Resolution* – A number of programs have written dispute resolution mechanisms in place. For example, if the Employee Assistance Program (EAP) or IG directors refuse to release information to the insider threat program, there is a higher-level official designated to make a final determination.

- *Continuous Review* – Most programs constantly evaluate the usefulness of particularly sensitive information. If a certain type of information is found to be of particular usefulness to an insider threat program, the offices engage to address what it would require to regularize access to that data.

EXTERNAL DATA SOURCES

After programs have effectively incorporated internal agency information into the program, insider threat programs can evaluate the value and feasibility of USG external data sources including but not limited to:

U.S. Travel Data

Reporting of U.S. border crossings and travel into and out of ports of entry. These data are particularly useful in detecting unreported foreign travel as well as providing illuminating additional details for self-reported travel.

Public Records Data

Could include arrests and detentions, bankruptcy, liens/holds, real property, vehicles, licensure (firearms, explosives, pilot, pharmaceutical), and some forms of social media. These data can often provide additional analytic insight into apparent anomalous conduct.

Financial Data

Provided by centralized credit reporting agencies, U.S. Treasury Financial Crimes Enforcement Network (FinCEN) reporting, and various other sources.

3. *Establish reporting guidelines for CI, Security, IA, HR, and other relevant organizational components to refer relevant insider threat information directly to the insider threat program.*

Meeting the Standard:

D/As establish written thresholds and processes for reporting information directly to the insider threat program. Personnel working in the relevant offices throughout the D/A are aware that when information reaches an established threshold it will be proactively referred to the insider threat program. The indicators and thresholds are tailored to that D/A's circumstances and socialized across the component to encourage maximum vigilance and reporting.

Best Practices:

- *Proactive Notification* – When a component identifies behaviors that are suspicious or meet the predefined indicator thresholds, it packages the relevant information and refers the matter to the insider threat program in an expeditious manner.

- *Collaboration* – Mature programs do not develop reporting guidelines in a vacuum. Instead, programs work with the relevant organizational components to collaboratively develop the reporting indicators and thresholds. This enhances relevance and encourages buy-in by the stakeholders and participating offices.

- *Risk-Based Approach* – Most D/As make a risk-based assessment of the reporting guidelines developed with the components. Programs prioritize indicators based on the value, volume, and time associated with the proactive notification while realizing that every D/A and every component therein will be different.

4. *Ensure insider threat programs have timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.*

Meeting the Standard:

Insider threat programs have timely access to finished intelligence production and counterintelligence information on adversarial threats. These sources of information provide context for an anomalous behavior, inform the insider threat program about evolving insider threat indicators, and educate insider threat programs about adversarial threats faced by its particular agency.

Best Practices:

- *Network Access* – Some insider threat programs have access to one or multiple classified networks that connect analysts/staff to portals and databases containing relevant reporting.

- *Briefer Approach* – Smaller insider threat programs have utilized a representative from its D/A intelligence office to become familiar with reporting on adversarial threats and brief the insider threat working group on relevant threats.

- *External Liaison* – The organizations with no access to classified networks, portals, or databases often establish agreements with other D/As that can provide updates on adversarial threats.

- *FSICs* – A number of Federal Partner D/As collaborate with their respective Federal Senior Intelligence Coordinators (FSICs) to obtain the necessary access to networks and information.

V. MONITORING USER ACTIVITY ON NETWORKS

1. MONITOR USER ACTIVITY ON ALL CLASSIFIED NETWORKS TO DETECT INDICATORS OF INSIDER THREAT BEHAVIOR.

2. POLICIES FOR PROTECTING, INTERPRETING, STORING, AND LIMITING ACCESS TO USER ACTIVITY MONITORING METHODS AND RESULTS.

3. AGREEMENTS SIGNED BY EMPLOYEES ACKNOWLEDGING USER ACTIVITY MONITORING.

4. CLASSIFIED AND UNCLASSIFIED NETWORK BANNERS INFORMING USERS ABOUT USER ACTIVITY MONITORING.

Agency heads shall ensure insider threat programs include:

1. *Either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLAs) shall be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs shall outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber's inside threat personnel.*

The monitoring of user activity on classified networks is a significant information source for insider threat programs and is conducted primarily via User Activity Monitoring (UAM) capabilities. Such solutions identify, analyze, and contextualize anomalous behaviors within the IT environment. As defined by the Committee on National Security Systems Directive 504 (CNSSD 504), UAM is "the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and support authorized investigations."

UAM is not simply a technical solution deployment. The NITTF views UAM as an action conducted by insider threat analysts. Users' network activity and behavior is captured, triaged, and presented in a human readable form, ideally in near real-time. UAM is a function of the program setting "triggers" as well as the criteria for monitoring, analyzing the results, and putting information into the proper context.

Meeting the Standard:

UAM solution(s) are implemented on all network endpoints that hold or access national security information (including stand-alone computers) while providing the following minimum capabilities to the insider threat program:

- Key stroke monitoring
- Capture of full application content (e.g., email, chat, data import, data export)
- Screen capture
- File shadowing for all lawful purposes
- Ability to set triggers/alerts based on user activity

USER ACTIVITY MONITORING (UAM) VS. ENTERPRISE AUDIT MANAGEMENT (EAM)

One common misconception is that EAM is synonymous with UAM. The two capabilities have many similarities, and elements of the two overlap. Although robust analysis of user-attributable enterprise audit can replicate many facets of UAM, EAM itself is not an adequate substitute. As the CNSSD 504 UAM definition states, UAM includes the capability to capture key strokes, screen shots, file content, and file shadowing, all elements beyond the scope of typical EAM.

How an agency implements UAM and thus meets the requirements will depend largely on whether the D/A is a classified network owner, subscriber, or provider:

- **Classified Network Owners**: D/As which own and operate classified networks implement UAM capabilities across all controlled classified domains/enclaves.

- **Classified Network Providers**: D/As which administer classified networks for other agencies are "providers." Providers are responsible for implementing UAM solutions on provided networks and formalizing UAM information-sharing relationships with subscribers through written agreement.

- **Classified Network Subscribers**: D/As which subscribe to classified networks and thus have no administrative control over such are considered to be "subscribers." Subscribers formalize UAM information-sharing relationships with their providers through written agreement.

Best Practices:

- *Singular Tool* – The majority of programs use one comprehensive UAM tool to meet all the technical requirements established in the *Policy & Standards* and CNNSD 504. Comprehensive UAM tools not only identify anomalous user behaviors, they help an insider threat program quickly and efficiently contextualize events. There are several Commercial-Off-The-Shelf (COTS) solutions that are compliant with these standards and approved for deployment on classified networks.

HARDWARE, SOFTWARE, AND TRANSPORT: WHAT DO I OWN?

Classified network "ownership" is a common source of confusion among D/As. The most common misconception is that an agency providing larger classified network connectivity is a provider under the minimum standards, and is therefore responsible for implementing a UAM solution. However, there are several D/As that provide classified network connectivity as a form of transport by providing the "pipes" in which packets of information travel between classified domains. In such cases, these D/As do not necessarily control, or even have visibility of the connected domains.

For the purposes of the minimum standards, network ownership means a D/A controls the classified domain/enclave and has administrative rights sufficient to deploy UAM software.

- *Multi-Tool Approach* – Some D/As have begun to address this requirement with a multi-tool approach. Programs have combined the capabilities inherent in various Security Information and Event Management (SIEM), Data Loss Prevention (DLP), enterprise forensics, network/application logging, and other cyber tools to meet the standards in aggregate. An insider threat program can be compliant if it has the capability to bring the data together from multiple tools, implement logical triggers, and detect anomalous activity indicative of insider threat behavior with fidelity required under CNSSD 504.

- *Video Capability* – Some D/As incorporate tools with near-real time "video" capability to view user activity as it happens at the endpoint, which can be invaluable in the resolution of anomalous events and inquires.

- *Operational Refinement* – More advanced insider threat programs incorporate statistical and mathematical review processes into UAM trigger development and deployment. This helps refine triggers and eliminate inefficient or ineffective collection.

- *OGC Review* – A close working relationship with OGC ensures triggers are legal and within policy.

- *Cross-Domain* – More mature programs have found it very useful to aggregate UAM across multiple network domains – moving UAM data to an enclave where the information can be aggregated and analyzed in its entirety. This is one method to quickly contextualize anomalous user behavior, thus creating a comprehensive view across all domains accessed by the user.

- *Enterprise Map* – The majority of programs have found it beneficial to create an IT enterprise map or topology displaying all of a D/A's classified networks, segments, endpoints, etc. to assist with UAM implementation planning. This effort usually requires extensive collaboration with the D/A CIO and CISO.

- *SAPS & Segments* – A number of D/As have initiated mitigation strategies to account for the difficulties in deploying UAM to some network segments, especially those involved with Special Access Programs (SAPs) and sensitive mission systems. D/As have implemented additional auditing and information assurance tools at the local level to gain more insight into user activity and lessen the vulnerability associated with gaps in coverage.

- *IT Planning* – Another recommendation is to incorporate UAM requirements into a D/A's IT planning, accreditation of systems, and design of future environments especially considering the USG push toward cloud technologies and common services.

- *MOAs* – Providers and subscribers of classified networks are using Memorandums of Agreement (MOAs) to formalize their UAM relationships with insider threat programs. Comprehensive MOAs often include a description of the UAM conducted by the provider, an outline of the mechanism by which the provider sends results to the subscriber, and articulation of the process for the subscriber to refine triggers/request more focused observation.

- *Collaboration* – Some subscribing insider threat programs also chose to share relevant threat and employee behavior information with the network provider to improve the detection of suspicious activity and more evenly distribute the risk between the two network partners.

- *Subscriber Access* – Subscriber insider threat programs should have as much direct access to UAM results as possible. Some providers offer the technical capacity for subscribers to perform their own review and analysis via role-based access to UAM dashboards and visualization modules. This allows the subscriber (which has more intimate knowledge of the users and organizational mission) to synthesize UAM results with other insider threat data elements to create additional context.

- *Unclassified Expansion* – Some insider threat programs have found that extending UAM capability to unclassified networks provides a deeper level of contextualization of anomalous behaviors and other detection benefits even though monitoring of unclassified networks is not specifically required by the *Policy & Standards*.
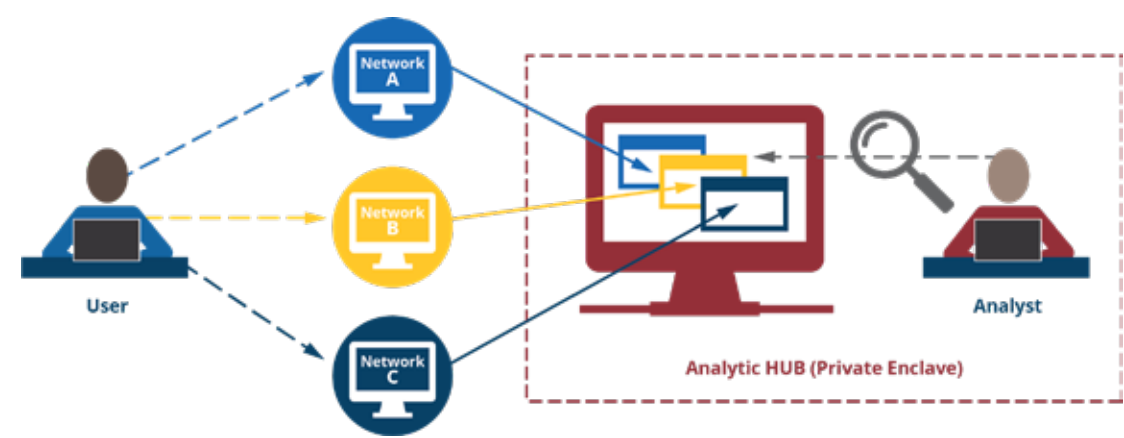
DEFINITIONS

RELATED TO UAM

Activity: Specific actions or functions that cause an interaction or change on the computer or network.

Agent: An UAM application running on a device that collects and reports UAM data.

Domain: An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Enclave: A set of systems resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Enterprise Audit (EA): An independent examination of records and activities, employed by the Chief Information Officer of a D/A, to assess the adequacy of system controls on computer systems operated by that agency and to ensure compliance with established policies and operational procedures.

Host: A host is an end-point device connected to a network and may offer information resources, services, and applications to other computers on the network.

Host-Based Software: In the UAM context, this is an application executed within the local computer configured by a central server to monitor user activity.

Trigger/policy: a set of logical statements to be applied to a data stream that produces an alert when an anomalous incident or behavior occurs.

Operational or Production System: The information and processing capabilities that support the daily operation of the organization in the accomplishment of its mission.

Service Level Agreement (SLA): A formal, negotiated document that defines in quantitative and qualitative terms the services being offered to a customer.

Service Provider: The D/A providing the classified network service to another D/A. The owner and operator of a classified system issued to and used by another D/A.

Subscriber: A D/A that accesses a classified network owned and managed by another D/A. A subscriber D/A likely has no granular visibility into their user's computer activity, as they do not technically administer the network.

User: Individual or (system) process acting on behalf of an individual, authorized to access an information system.

2. *Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.*

Meeting the Standard:

D/A has documented physical, personnel, and information security controls in place to prevent the unauthorized access or disclosure of UAM methods and results. UAM data often includes highly sensitive data such as PII or information that might damage an individual's reputation. Such data must be properly stored, safeguarded, and limited to those individuals with a legitimate need to know.

Best Practices:

- *NDAs* – The majority of D/As utilize Non-Disclosure Agreements (NDAs) for insider threat program personnel with access to UAM method and results. The NDAs clearly delineate acceptable uses and restrict the disclosure of UAM capabilities and monitoring data.

- *IA Support* – Additional measures have been taken by smaller programs in which IA components have assigned personnel to hubs in order to implement UAM, conduct system design activities, or perform technical analysis. In such cases, steps must be taken to ensure that these personnel operate under the strict management of the insider threat program and do not share their knowledge of UAM capabilities to those not authorized to receive it.

- *Storage* – It is recommended that the collection and storage of UAM data should be done in accordance with all applicable laws and policies to avoid conflict with privacy and civil liberty laws. The parameters are developed in collaboration with OGC and incorporated into the larger insider threat program implementation plan.

- *Classification* – UAM data classification should be equal to the highest classification from which the data was obtained.

- *Independence* – Some mature programs operate with some measure of separation and independence from IA and CIO elements help enhance the insider threat program's ability to detect, deter, and mitigate insider threats from privileged users when necessary.

- *Private Enclaves* – A number of programs utilize private network enclaves to store UAM data thus segregating this sensitive data from the larger enterprise to provide extra layers of access control and information protection.

- *Watch the Watchers* – Several programs have developed sophisticated systems and processes for supervisors, peers, and even 3rd party staff to review the activities of UAM analysts to ensure they are staying within the proper legal and ethical boundaries of their duties.

SENSITIVE NATURE OF THE UAM PLAN

The UAM plan should be classified. Details of the plan, particularly the logic, may reveal tactics, techniques, and procedures and may need to be classified. Some agencies will conduct UAM on unclassified networks. For those agencies, the implementation of a UAM plan on an unclassified network should be protected in a manner to prevent disclosure of classified information.

The program should limit and control the persons that have knowledge of the UAM plan. Ideally, only a few people on the program will know all the details of the plan. The details of the plan, especially advanced logic, should NOT be shared with anyone outside the program, particularly the CIO staff. The CIO staff will be the ones responsible for deploying the software and will have the highest concentration of privileged users under their area(s). Privileged users typically have a great deal of access to data and systems in IT environments and should be subject to an additional degree of monitoring.

3. *Agreements signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel.*

Meeting the Standards:

All cleared D/A personnel (to include staff employees, contractors, and assigned military personnel) sign a pre-approved user agreement(s) that acknowledges their activity is subject to monitoring and can be used against them. This can be done via an electronic acknowledgment or signature. The agreement provides a sufficient legal framework to include all D/A classified or unclassified networks including portable electronic devices. The language of the user agreement is approved by the insider threat program senior official and OGC to ensure the language can withstand scrutiny in a criminal, security, or administrative proceeding. The insider threat program also has the ability to verify that all cleared personnel have signed the user agreement(s).

Best Practices:

Contact the NITTF for sample user agreements.

4. *Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be approved by the Senior Official(s) in consultation with legal counsel.*

Meeting the Standards:

D/A network banners provide the sufficient legal framework for the monitoring of user activity and subsequent D/A actions as a result of such monitoring. Language includes statements that the network is owned by the U.S. Government, that the user understands there is no expectation of privacy on the network, and that the user is aware of, and consents to monitoring. Further, the language advises the user that the Government may take administrative, civil, and/or criminal action as a result of improper use.

Best Practices:

The Department of Justice (DOJ) established specific language for network banners.

> (2) WARNING! This computer system is the property of the United States Department of Justice and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit.

THE MONITORING OF USER ACTIVITY ON CLASSIFIED NETWORKS IS A SIGNIFICANT INFORMATION SOURCE FOR INSIDER THREAT PROGRAMS.

VI. INFORMATION INTEGRATION, ANALYSIS AND RESPONSE

1. BUILD AND MAINTAIN INSIDER THREAT ANALYTIC AND RESPONSE CAPABILITY.

2. ESTABLISH PROCEDURES FOR INSIDER THREAT RESPONSE ACTIONS.

3. DEVELOP GUIDELINES AND PROCEDURES FOR DOCUMENTING INSIDER THREAT MATTERS.

Agency heads shall:

1. *Build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate.*

The final category builds upon all of the previously introduced minimum standards and serves as a culminating function for an operational insider threat program. While behavioral anomalies detected as a result of Access to Information, the Monitoring of User Activity, and reporting from Employee Awareness & Training are important, maximum value is gained only when disparate information points are fused together to identify intricate patterns of conduct that may be unusual or indicative of insider threat activity. The analysis of gathered information from multiple sources creates a picture of employee activity that may not be available or apparent by reviewing information from only a single source. This centralized synthesis and analysis, when combined with methodical response procedures, sets the conditions for the proactive and early detection of insider threats.
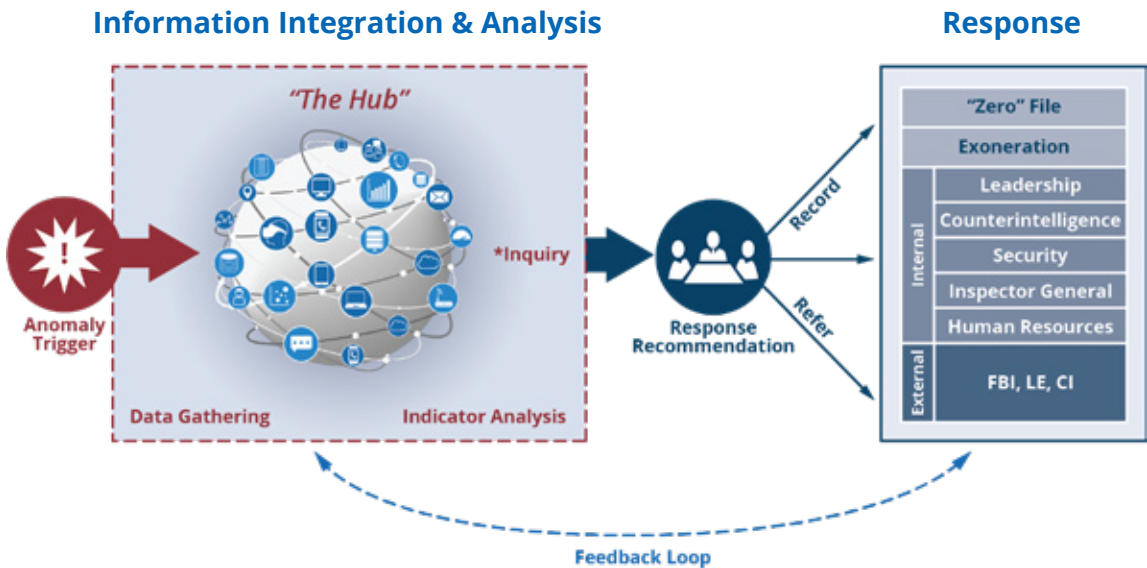
Meeting the Standard:

Insider threat relevant information from all appropriate D/A components and sources is gathered, integrated, and analyzed in a centralized fashion to facilitate detection of insider threat behavioral anomalies. While D/As can consolidate and automate these mechanisms as much as possible, a program can minimally comply with this standard using a working group and manual processes. For example, insider threat representatives from different D/A components might assemble and bring hard copy information on a potential issue. The fundamental key is to merge disparate information and differing functional perspectives to view indicators more holistically and move toward a proactive detection strategy.

Best Practices:

- *Hubs* – Information, analysis, and response functions are typically conducted within an insider threat "hub."

- *Centralized Capabilities* – Some organizations establish their hub as only a centralized analytical capability or information repository. However, more mature programs also use the hub to consolidate activities and ensure that an appropriate action is conducted to resolve the concern. Some D/As use alternative names for hubs including office, center, branch, etc.

- *De-confliction* – A number of D/As with significant security, counterintelligence, and investigative capabilities take extra measures to share and de-conflict some of these functions with the hubs. It is critical to ensure that in such scenarios, access to insider threat information is strictly controlled, coordinated appropriately, and responsive to the insider threat program and senior official(s).

- *Sharing Arrangements* – Most D/As leverage their working groups and senior leadership from component offices to assist the hub in identifying which information should "flow" into the hub. It is critical to define and continually refine these relationships based on an understanding of what information resides in the various agency offices, what content is of analytic value, and what legal coordination may be necessary.

- *Quality Reviews* – Mature hubs institute a quality assurance/control process to periodically review the quality and quantity of information originating from a particular source or office. This helps a hub determine data filters and boundaries to help prevent floods of non-relevant information. In these situations, relevant details may get lost in the large volume of data while anomaly patterns become obscured.

- *Digital Pushes* – Hubs should acquire and gather relevant information in digital format whenever possible. This increases the quantities of data and facilitates the integration and correlation of data for analytical purposes.

- *Automation* – Programs should strive to automate the processes to acquire and gather relevant information from component sources. This allows hubs to receive data with predictable frequency and lessens the resource burden on hub staff to coordinate and acquire the information.

- *Hub Personnel* – Some programs designate staff to serve as insider threat analysts and provide training to help develop pertinent skills and competencies. This includes the ability to link disparate pieces of multi-functional information (intelligence reports, security records, IA logs, HR files) into a mosaic contextualizing anomalous behavior.

- *Behavioral Science* – A number of programs incorporate behavioral science perspectives and expertise into hub activities. Behavioral science experts provide insights into employee motivations, behaviors, and social/cultural environments. These additional viewpoints assist hubs in conducting analysis, in refining indicators/triggers, and in conducting inquiries/response activities.

- *Analytic Horsepower* – Several of the more mature hubs use analytic engines and software to enhance analysts' capacity to review and triage large amounts of information. Such tools expedite the correlation of information and help prioritize indicators so that analysts can focus attention on the most alarming issues.

- *Geographic Dispersion* – In a few cases, larger organizations with multiple subordinate elements or numerous facilities spread over a wide geographical area have chosen to establish multiple analytic centers linked by a central information repository. Operations may occur in physically separate locations but are coordinated and managed centrally.

FOUR STEPS

TO IMPLEMENTING A HUB

1. Identify what agency components are likely to possess information of insider threat interest.

2. Collaborate with each component individually to determine what information would be useful to detect behavioral anomalies.

   – Understand the possible insider threat indicators that various information can provide.

   – Determine that the consolidation and forwarding of information to the hub will maintain the protection of civil liberties and privacy and is consistent with: federal statutes; executive orders; presidential directives; agency policy; and, for the IC, Attorney General-approved guidelines for the collection, retention, and dissemination of information concerning United States persons.

3. Hub and components should determine how relevant data can efficiently flow to the hub.

   – Will the information flow to the hub digitally or through manual means employing actual human interface with the information?

   – If digitally, will it be an automated push? In what format? What will be the frequency of updates?

   – If manually, is there a discreet process for hub personnel to obtain needed information in a timely manner?

4. Determine how you will staff the hub.

   – Will it be composed of full-time, dedicated, discipline-agnostic staff?

   – Will it be composed of assignees from the various D/A components?

   – Will it be composed of part-time liaisons from the various D/A components?

2. *Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the insider threat program within the agency or one of its subordinate entities.*

Meeting the Standard:

D/As establish written and approved response procedures for responding to insider threat matters. The written procedures will ensure that inquiries are conducted within proper limits, the individual's privacy and civil liberties are protected, whistleblower protections are enforced, and that the inquiry does not taint evidence or jeopardize a possible investigation or prosecution by a law enforcement agency. D/A policies set the conditions for matters to be reviewed fairly, consistently, thoroughly, and in accordance with applicable laws and regulations. Response actions are centrally managed to ensure all necessary stakeholders have appropriate situational awareness, involvement, and oversight so that all D/A response actions remain within the bounds of legal and regulatory authorities.

Best Practices:

- *Alert Triaging* – A number of hubs respond to a significant insider threat indicator or behavioral anomaly with additional scrutiny through a triage process to further validate information and clarify the circumstances of detected activity.

- *Inquiries* – When an alert or indicator meets a designated threshold of concern, some programs initiate a preliminary inquiry to formalize response actions. These inquiries can be conducted by insider threat personnel or referred to a separate office of trained investigators. Such designation is specified in the agency insider threat policy and within guidelines that detail the investigative procedures and authorities.

- *Investigative Referrals* – Close coordination should occur among the hub, the OGC, and law enforcement/CI components with investigative authority to determine the appropriate thresholds for transfer when a preliminary inquiry reaches the point of maturity or concern that it should be referred to another entity.

- *811 Referrals* – D/A hubs and programs should establish substantive working relationships with the appropriate FBI offices and be familiar with the 811 referral process. This will expedite coordination during future 811 referrals and help safeguard the admissibility as evidence of any agency-developed information in the event a matter reaches the level of a legal prosecution.

- *Internal Referrals* – It is recommended that Hubs establish written guidelines outlining the referral of lesser matters to various D/As components once the hub has completed an inquiry and exhausted all of its analytic capabilities. Some D/As coordinate with their internal Security, HR, IG, Employee Assistance, and other offices for response reconciliation.

- *Issue Resolution* – Most D/As continue to monitor the status of external referrals to track final disposition and receive timely feedback on the outcome. Such input drives hub process improvements and training of insider threat detection personnel.

- *Feedback Loops* – A number of programs establish formal feedback loops from responders back to the hub to keep insider threat programs informed of resolution of matters, to request clarifying information, and to aid de-confliction among internal and external stakeholders.

- *Whistleblower Protection* – Most D/As emphasize whistleblower protections in their documented response actions to ensure that they do not inadvertently enable retaliation against employees for protected classified communications.

WHISTLEBLOWER PROTECTIONS

There are statutory and regulatory provisions that apply to agencies to encourage employees to disclose suspected incidents of fraud, waste, and abuse and to protect those who make such disclosures from retaliation. Agencies should collect, review and incorporate the federal authorities relating to lawful whistleblowing, as opposed to the unlawful act of leaking. A lawful disclosure is to a person or an entity allowed by law to receive the disclosure. Programs at intelligence agencies, the DoD, or federal partner agencies should work with their general counsel to understand what whistleblower authorities and regulations apply to their D/A. D/As should also include content in their agency insider threat program training that will aid supervisors, managers, and employees in understanding the difference between lawful whistleblowing and unlawful leaking.

3. *Develop guidelines and procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of each matter.*

Meeting the Standard:

Programs have established written and approved procedures to maintain documented records of detected indicators and response actions in order to track hub activity, reinforce accountability for timely resolution, and establish analytical trends and baselines. The procedures specify what aspects of the inquiry must be documented, in what format, and what approvals are needed before proceeding to successive steps. Programs also must demonstrate a methodology for tracking insider threat matters and response actions.

Best Practices:

- *Case Management Tools* – Mature insider threat programs typically utilize case management or workflow solutions to enhance the tracking and documentation of activity in light of large information volumes distributed across multiple analysts/investigators.

- *Flowcharts* – Many programs develop a diagram or chart illustrating the flow of response actions and procedures.

- *Safeguarding* – D/As take significant measures to secure and back-up such case management databases or files because they quickly become valuable yet sensitive data sources for contextualizing anomalous behaviors previously reviewed by the hub.

- *Geographic Dispersion* – In some D/As, response activity occurs at multiple physical locations as long as there is a process to track, oversee, and management response actions emphasizing the protection of the evidentiary chain and the privacy and civil liberties of all individuals.

- *Deadlines* – Most programs establish time guidelines for conducting inquiries and various response actions to ensure matters are addressed and resolved in a timely manner.

MAXIMUM VALUE IS GAINED ONLY WHEN DISPARATE INFORMATION POINTS ARE FUSED TOGETHER TO IDENTIFY INTRICATE PATTERNS OF CONDUCT THAT MAY BE UNUSUAL OR INDICATIVE OF INSIDER THREAT ACTIVITY.

THE NITTF HOPES THE INSIGHTS
WITHIN THIS COMPENDIUM OFFER
D/As INNOVATIVE AND VALUABLE
WAYS TO ADDRESS CHALLENGES,
ENHANCE CAPABILITIES, ULTIMATELY
COMPLY WITH ALL PROGRAMMATIC
REQUIREMENTS, AND EVEN GO
ABOVE AND BEYOND THE MINIMUM
STANDARDS WHEN APPROPRIATE.

2017 INSIDER THREAT GUIDE