



GUIDE

TO ACCOMPANY THE NATIONAL INSIDER THREAT POLICY AND MINIMUM STANDARDS

OCTOBER 2013



UNCLASSIFIED//~~FOUO~~

(U) Table of Contents

- (U) **INTRODUCTION**1
- (U) **HELPFUL REFERENCES**3
- (U) **TO BEGIN . . . DEVELOPING AN INSIDER THREAT POLICY AND IMPLEMENTATION PLAN**5
 - (U) Step 1: Designate the Senior Official.....5
 - (U) Step 2: Obtain Visible Support from the Agency Head5
 - (U) Step 3: Form Working Group/Periodic Feedback to the Community.....5
 - (U) Figure 1: Insider Threat Program: Enterprise View**.....6
 - (U) Step 4: Review Current Requirements and Guidance9
 - (U) Step 5: Seek Legal Input 11
 - (U) Step 6: Protect Privacy and Civil Liberties by Applying Appropriate Safeguards 11
 - (U) Step 7: Identify Classified and Other Critical Assets 12
 - (U) Step 8: Write Agency Policy and Implementation Plan..... 13
 - (U) Step 9: Obtain Approval, Establish Program Office, Implement Plan..... 14
 - (U) Step 10: Conduct Scheduled Self-assessments 15
- (U) **IMPLEMENTING THE POLICY AND STANDARDS**17
 - (U) Responsibilities of Senior Official(s) 17
 - (U) Information Integration, Analysis, and Response20
 - (U) Insider Threat Program Personnel.....27
 - (U) Access to Information31
 - (U) Employee Training and Awareness34
 - (U//~~FOUO~~) Implementing a Host-Based User Activity Monitoring (UAM) Capability35
 - (U//~~FOUO~~) Figure 2: User Activity Monitoring (UAM)**36

(U) Step 1: Review Policies40

(U) Step 2: Evaluate the Current Underlying Information Technology Environment.....40

(U) Step 4: Establish the UAM Capability41

(U) Step 5: Identify, Evaluate, and Prioritize Concerning Insider Threat Conduct43

~~(U//FOUO)~~ **Figure 3: Malicious Behavior**.....**44**

(U) Step 6: Develop an Information-Gathering Plan44

~~(U//FOUO)~~ Step 8: Send Data to the Program Hub47

(U) Step 9: Oversight48

(U) **Appendix A:** Guidelines for Media Interface51

(U) **Appendix B:** Agency Policy Template54

(U) **Appendix C:** Agency Implementation Plan Template.....59

(U) **Appendix D:** Insider Threat Priority Area Questionnaire.....65

(U) **Appendix E:** 811 Referral Template68

(U) **Appendix F:** Insider Threat Classification Guide (to be published)69

(U) Notes.....70

UNCLASSIFIED//~~FOUO~~

(U) INTRODUCTION

(U) Executive Order (E.O.) 13587, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, in conjunction with the White House Memorandum on *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (hereinafter “Policy and Standards”), direct all executive branch departments and agencies (hereinafter “agency, agencies”) that have access to classified information to implement an insider threat detection and prevention program (hereinafter “Program”). The purpose of the Program is to deter, detect, and mitigate insider threats. This *Guide* provides instructions, ideas, and possible options to assist agencies as they establish and tailor a Program to meet their particular needs.

(U) The Program requirements contained in the E.O. 13587 and the Policy and Standards extend beyond the safeguarding of information on computer networks and systems. By the definition contained in the Policy and Standards, insider threat requires the establishment of capabilities that apply to classified information in all its forms, including information stored electronically or contained on systems as well as to the activities of persons who use that information. For that reason, an agency Program will be required to implement standards that apply to computer usage and system access, and encompass detection, prevention, and reporting capabilities that cover information that resides outside the network environment.

(U) Agency heads are responsible for approving the agency’s insider threat policy, establishing a Program, and promulgating additional agency guidance, if needed; designating a Senior Official responsible for the Program; establishing a user activity monitoring

capability; ensuring access by Program personnel to insider threat-related information and data drawn from across the agency; ensuring legal, privacy, civil rights, and civil liberty issues are addressed; establishing a centralized capability to analyze that information and to direct appropriate agency responses to insider concerns; performing agency self-assessments of compliance with the Policy and Standards; reporting results of agency insider threat efforts to a Senior Information Sharing and Safeguarding Steering Committee (SC), as established by executive order; and enabling independent assessments of agency compliance.

(U) The E.O. 13587 applies only to the safeguarding and sharing of classified national security information and information that is classified under the *Atomic Energy Act of 1954*. The National Insider Threat Task Force (NITTF) recognizes, however, that an agency may possess information that it considers sensitive but that is not classified. While the principles and practices discussed herein are written to help agencies execute the E.O. 13587 and the Policy and Standards, they can be applied generally to protect a sensitive but unclassified environment.

(U) To ensure that Program activities are conducted within legal authorities, this *Guide* emphasizes the value of close collaboration with agency counsel and agency privacy and civil liberties officials. The acquisition and use of personal information to detect and prevent insider threats is permitted under the E.O. 13587 and other national policies. Collected information is subject to oversight by civil liberties and privacy authorities to ensure that personally identifiable information is only gathered and used for legitimate and authorized purposes; such information must be strictly controlled within the Program.

UNCLASSIFIED//~~FOUO~~

(U) In establishing their Programs, agencies are expected to implement the Policy and Standards. All minimum standards must be met, but that does not mean that Programs should necessarily remain static or that a solution that works for one agency will necessarily work well for another. A “one size fits all” model for the federal government is not required. Agencies are provided a great deal of latitude to develop a Program tailored to their unique organization and mission, capabilities, resources, and, most importantly, its perception of the threat from malicious insiders. As an agency sets its own path toward compliance, it should bear in mind that the Policy and Standards are only minimums. Agencies will want to periodically evaluate and reassess their insider threat posture. This may result in an agency’s determination that they should raise their standards, even above those set in the minimum standards.

(U) There is no single right solution to insider threat detection and prevention: each agency must determine its own pathway to accommodate its specific environment and resource priorities, while implementing the Policy and Standards.

(U) This *Guide* begins with a compilation of useful references (see *Helpful References, page 3*), followed by a discussion of the steps (see *To Begin...Developing an Insider Threat Policy and Implementation Plan, page 5*) needed to implement a functional insider

threat program for agencies that have not yet instituted their Programs. Finally, each minimum standard is discussed (see *Implementing the Policy and Standards, page 17*) with a view toward providing helpful tools and techniques that an agency can employ to deter, detect, and mitigate malicious insider activity.

(U) Some redundancy and repetition has been intentionally woven into the *Guide* to reinforce important themes as they appear in different contexts throughout the *Guide*. For example, a point—such as the need for collaboration among various agency stakeholders—may be pertinent in the context of the Policy and Standards, may play a role in the analysis of information, may be significant from the perspective of protecting the privacy of personal information, is certainly an important consideration for an agency insider threat working group to consider, and may be important to an agency’s insider threat training program. Collaboration, then, as a theme is discussed in each of those contexts.

(U) Questions about the classification of insider threat materials are anticipated. To assist, the NITTF is preparing a classification guide for insider threat-related activities and materials that will answer questions about the proper classification of insider threat information. Upon completion, it will be disseminated to all agencies that handle classified information and added as an appendix to this document.

UNCLASSIFIED//~~FOUO~~

(U) HELPFUL REFERENCES

(U) Several useful references warrant mentioning.

(U) First, 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. These national policies direct all executive branch departments and agencies (hereinafter "agency, agencies") to implement insider threat detection prevent programs.

(U) Second, an agency must understand that it already possesses the authority to investigate any information that comes to its attention that indicates retaining any officer or employee of the agency may not be consistent with national security interests. This investigative authority is contained in **E.O. 10450, *Security Requirements for Government Employment***, as amended, and provides authority to conduct inquires both prior to an actual hiring and after an individual has been hired by the agency.

(U) Third, the FBI Office of General Counsel has assembled a ***Summary of Federal Citations for the National Insider Threat Task Force***. This document provides extensive authorities, derived from U.S. law and policy, that pertain to insider threat activities. Reference materials have been extracted from the United States Code, executive orders, Code of Federal Regulations, presidential national security and homeland security directives, intelligence community directives and standards.

The references provide a ready resource for agency counsel, privacy and civil liberties coordinators, Program personnel, and agency leaders.

(U) Fourth, although the structure and purposes of a Program can be applied readily to sensitive information that is not classified, the focus of E.O. 13587 is on improving the safeguards associated with 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***, 4 August 1995 and to section 3 of **E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified national Security Information***, 30 June 2008.

(U) Fifth, 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*** at www.nrc.gov/about-nrc/governing-laws (unclassified)).

(U) Sixth, 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. Modifications to the National Industrial Security Program are presently being drafted within the executive branch to specifically apply the Policy and Standards to the cleared contractor workforce.

(U) Seventh, the NITTF encourages agencies that do not yet have CI capabilities to develop those capabilities concurrently with their Program. The two will be mutually reinforcing. This suggestion is

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

consistent with E.O. 13587, which requires that the government-wide Insider Threat Program develop policies, objectives, and priorities for counterintelligence capabilities and practices within agencies. CI capabilities are outlined in the *Defensive Counterintelligence Program Blueprint—2010*. An important component of any CI capability is the agency commitment to periodically assess the risks posed by adversaries to agency critical assets. Office of the National Counterintelligence Executive (ONCIX) has recently published an instructional manual, *Counterintelligence/ Security Risk Assessment Framework for Federal Partners*, March 2012, which agencies should find useful in conducting a CI risk assessment.

(U) Eighth, in December 2012, Carnegie Mellon University Software Engineering Institute's CERT Program published a useful unclassified reference document on insider threat entitled *A Common Sense Guide to Mitigating Insider Threats, 4th Edition*. The guide provides nineteen positive practices drawn from CERT's experience working insider threat situations over the past decade. The practices, supplemented by case studies and examples, can help agencies formulate their own programs and provide materials for the insider threat awareness training component of their Program. Also in 2012, CERT published its unclassified *CERT Guide To Insider Threats* (available from CERT at http://www.cert.org/insider_threat), which provides numerous case studies of malicious insider activities drawn largely from private sector examples.

(U) Ninth, there are two recent documents that deal specifically with the components of insider threat programs. First is the National Insider Threat Working Group's *U.S. Government Insider Threat Detection Guide, 2011*;^a its contents closely parallel the Policy and Standards and this *Guide*. Second is ONCIX's *Insider Threat Concept of Operations (CONOPS), 2011*.^a

(U) Tenth, most agencies possess a document or charter, issued at the time the agency was initially organized, that established the mission and its operational parameters. This charter should be reviewed for possible guidance and authorities that an agency can incorporate into its Program.

(U) Eleventh, behavioral science specialists may serve as a valuable resource in defining conduct indicative of insider threat concern. Additional information on deployment of behavioral science expertise may be found on the ONCIX classified website (b)(3)

Two related other publications are the University of Nebraska's *Behavioral Science Guidelines for Assessing Insider Threats*, which was published in 2008 for the Department of Defense (DoD), and ONCIX's *Counterproductive Work Behavior and Resilience*, August 2012.

(U) Twelfth, NITTF recommends the employment of security, information security, and counterintelligence skills prominently within an agency's Program. The IC and the DoD have done considerable work to outline the competencies in these skill areas. Agencies, regardless of whether they are part of the IC, may find useful the skill descriptions developed in the following documents:

- Office of the Director of National Intelligence's (ODNI) *Intelligence Community Standard (ICS) 610-13, Competency Directory for Security*, 4 October 2010;
- ONCIX's *Fundamental Elements of the Counterintelligence Discipline, Technical Competencies for Counterintelligence Functions, Volume 2*, 1 August 2007;
- ODNI's *ICS 610-9, Competency Directory for Information Technology (Mission and Enterprise)*, amended 4 October 2010;
- DoD's *Department of Defense Manual 8570.1-M, Information Assurance Workforce Improvement Program, Change 3*, 24 January 2012.

(U) Most of these references are retrievable through links provided the electronic version this *Guide*. Eventually these and other materials will be available on classified and unclassified websites that the NITTF is presently constructing. All of the materials may also be requested by contacting the NITTF via e-mail at (b)(3) (classified) or (b)(3) (unclassified).

^a This is classified document.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) TO BEGIN . . . DEVELOPING AN INSIDER THREAT POLICY AND IMPLEMENTATION PLAN

(U) The following ten steps should be implemented when developing a functional insider threat program. The steps cover the insider threat minimum standards contained in the president's memorandum of 21 November 2012. These steps are comprehensive and designed for agencies that have not yet instituted an Insider Threat Program. Figure 1: Insider Threat Program: Enterprise View (see page 6) illustrates the primary roles, E.O.s, policy, systems and data sources that are needed for an Insider Threat Program.

(U) Step 1: Designate the Senior Official

(U//~~FOUO~~) Agencies are required to designate a Senior Official responsible to the agency head for implementing and overseeing the Program. Recommend only one official be designated to manage and oversee the Program; however, if an agency appoints more than one Senior Official (such as in the case where an agency has many subordinate elements or multiple geographically separated facilities), a coordination process should be established so that the Program speaks with one voice. The Senior Official should have direct access to the agency head for matters of insider threat concern. It is recommended that the Senior Official's performance plan reflect this responsibility. In a number of agencies with maturing Programs, the responsibility for the Program is vested in a senior executive who is also responsible for the agency's security and/or counterintelligence 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 structure of the agency. Additionally, the pursuit

of insider threats is a security concern, making the association between the Program and the agency's security structure natural and mutually reinforcing.

(U) Step 2: Obtain Visible Support from the Agency Head

(U//~~FOUO~~) Along with the designation of the Senior Official, the agency head should demonstrate strong, personal, and visible support for the new Program and its senior responsible official.

(U) The agency 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 in use by the agency head and can be effective communication vehicles through which the agency head can frame and emphasize the agency insider threat discussion.

(U) Agency heads who are visibly involved in Program awareness provide a valuable level of emphasis to the workforce; leadership endorsement of the Program is also greatly enhanced when agency heads lend their name and/or image in workforce communications about the Program.

(U) Step 3: Form Working Group/Periodic Feedback to the Community

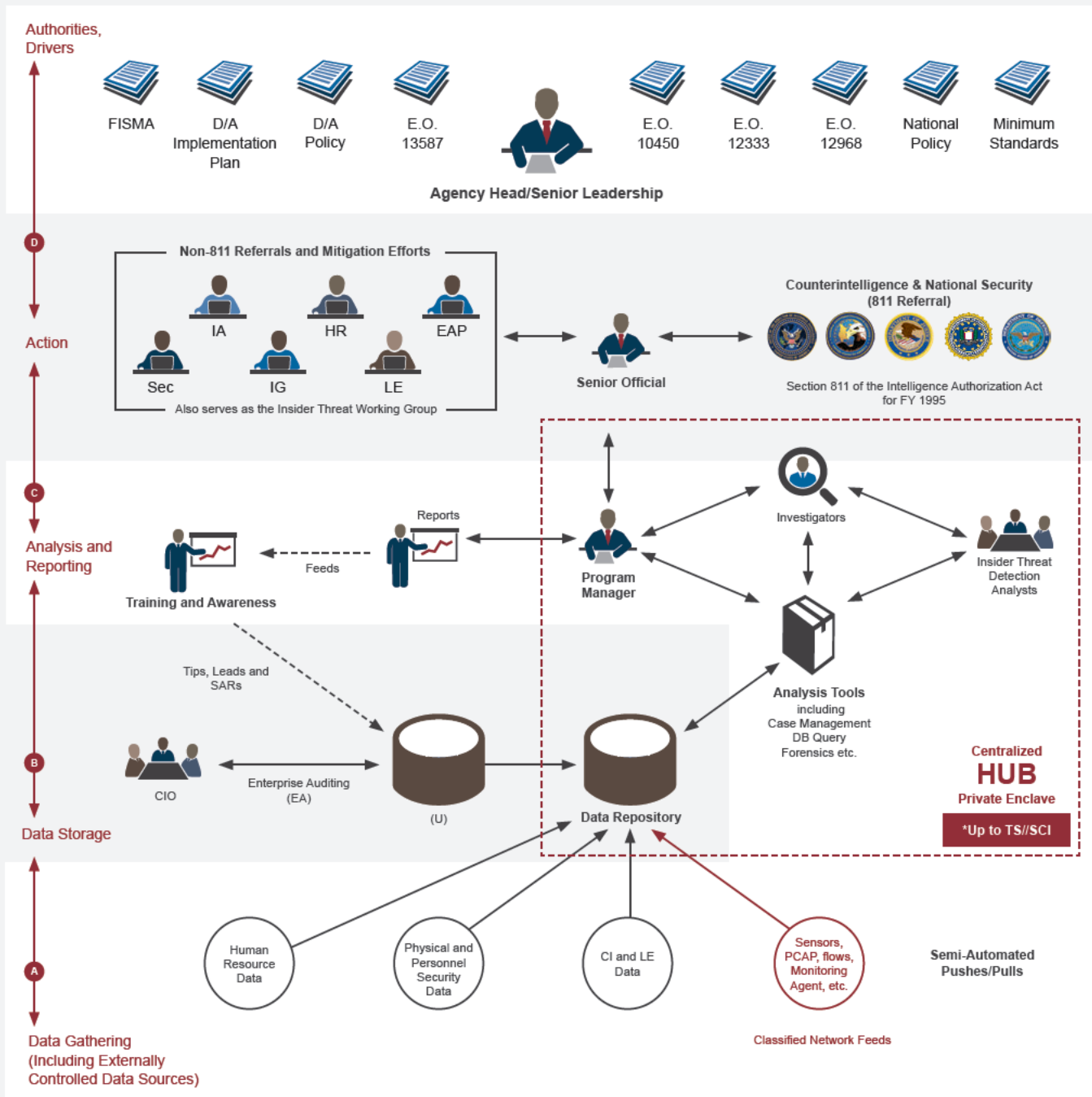
(U//~~FOUO~~) Once designated, the Senior Official may wish to assemble an ad hoc cross-agency working group that will meet regularly over the months ahead to develop the Program and implement the Policy and Standards. The Senior Official should consider providing in-person periodic updates to the agency head and leadership on the group's progress. This interaction will serve to reinforce senior leadership

UNCLASSIFIED//~~FOUO~~



(U) Figure 1: Insider Threat Program: Enterprise View

This graphic is (U//~~FOUO~~).



SARs=Suspicious Activity Reports.

(U//~~FOUO~~) The figure is an overview at the enterprise level of the interrelationships among the various components of a typical insider threat program discussed in this Guide.

UNCLASSIFIED//~~FOUO~~

(U//~~FOUO~~) Questions for the Insider Threat Working Group

(U//~~FOUO~~) The working group should consider the following during its discussion

- What are we trying to protect?
- How will the Program be implemented and over what period of time?
- Who will write the policy and implementation plan?
- When can we reach initial operating capability (IOC)/ full operating capability (FOC)?
- What capabilities are in place within the agency that will contribute to the Program?
- What capabilities are missing? What is needed?
- What information resources in the agency will be useful to the Program? Where do they reside in the agency? Are the “keepers” of that information involved in the working group?
- What possible vehicles does the agency have to promulgate a Program policy?
- How will the Program deal with subordinate elements and/or elements that are geographically removed from the agency headquarters? Will there be a need for several “senior responsible officials”?
- How will the agency fund and staff a Program office to implement the agency’s insider threat policy?
- How and where will the agency’s “hub” or centralized analysis and response capability be established? Will there need to be several “hubs” to service the agency’s needs? How will their information interconnect?
- What action can and should the agency undertake to apply its insider threat policy to its contractor workforce and personnel located in remote locations?
- Determine what safeguards should be included in the Program to ensure the protection of insider threat information and the civil liberties and privacy of individuals.

awareness of and support for the Program and allow the agency head to incorporate the positive results of the Program development effort into his/her portrayal of the agency’s status and posture. The working group can also help to develop relationships between components/offices, leading to better information sharing and cooperation. This also will serve to minimize 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.

(U) 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. As a rule of thumb, stakeholders would certainly include representatives from the security/counterintelligence staff, the Office of the Inspector General (OIG), the law enforcement elements of the agency, the Human Resources (HR) office, the Information Assurance (IA) Office, and the Office of the Chief Information Officer (CIO). However, any office within the agency that possesses information about the activities of agency employees could be considered a stakeholder for purposes of the working group. In short, tailor the working group to your agency.

(U) Critically, the Office of the General Counsel (OGC), Solicitor General, or Corporation Counsel should be included as a working group member in order to help sort through questions that may arise about authorities and legal impediments. Civil liberties and privacy office(s) should also be represented. As the agency 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. *(See Summary of Federal Citations for the National Insider Threat Task Force, page 3.)*

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) The broad membership of the working group should guarantee wide input from across the agency, which in itself should be seen as an advantage for the Program and should assist in familiarizing the agency staff leaders with the requirements of the Policy and Standards.

(U) It should be emphasized that the Policy and Standards address agency actions that should apply to their employees; the definitions of “employee” and “cleared employee” contained in the Policy and 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 and Standards into the provisions of the agency’s commercial contracts that involve classified information and access by contract personnel to that information. As this *Guide* is being written, efforts are under way to modify the *National Industrial Security Program Operating Manual* (NISPOM) and implementing guidance, which govern access to classified information by contract personnel, to expressly apply the Policy and Standards to the contract workforce.

(U) 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 agency 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 agency 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 national security guidance found in the NISPOM. All agencies with cleared contractors must follow the security programs established by their respective CSAs.

(U) As the agency insider threat working group reviews the various requirements and guidance that applies, the working group, with agency counsel participation, should take care to initiate a dialogue with their CSAs to ensure that, at the appropriate time, the Policy and Standards are applied to the agency’s 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 contractors? This discussion may also require contact with service providers (see page 42) from other organizations when those organizations operate classified computer systems and networks that the agency uses (see *Implementing a Host-Based User Activity Monitoring Capability*, page 35).
- 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 (i.e., the “hub;” see *Centralized Hub: Information Analysis and Response*, page 20) required by the Policy and 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 and Standards apply to information held by the contracting firm?
- Are there records retention issues to consider when the records contain contractor information?

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) In addition, the working group may wish to keep the workforce informed about Program developments to reduce rumors and employee misconceptions. The agency probably has established means for disseminating important information to the workforce, perhaps through newsletters, leadership e-mails, and “all hands” or large group meetings. Such vehicles can serve the dual purpose of keeping the workforce informed about the Program while encouraging a sense of insider threat awareness. These same communications forums also can serve to convey Program emphasis by the agency head.

(U) The working group or the agency may receive external queries pertaining to the work of the NITTF and E.O. 13587. Refer these queries to NITTF

(b)(3) the FBI Public Affairs Office (b)(6) or the ODNI Public Affairs Office (b)(3). A communication guide (see Appendix A, page 51) is provide to assist with and to respond to external queries.

(U) Step 4: Review Current Requirements and Guidance

(U//~~FOUO~~) The working group should identify policies and procedures that are already in place within the agency, which 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 and Standards. These discussions of the agency’s particular environment will help the working group to tailor its Program to meet the distinct needs, mission, and systems of the agency; guarantee privacy, civil rights, and civil liberties of agency personnel; and accomplish the president’s insider threat objectives. Agency responses to the Key Information Sharing and Safeguarding Indicators (KISSI) (see Appendix D, page 65) may offer a useful measure of agency insider threat capabilities for the working group’s discussion.

(U) Access to Information

(U) The working group should identify offices within the agency that possess information needed for insider threat analysis. The agency’s policy and implementation plan (see Appendix B, page 54 and Appendix C, page 59 for templates) should include sufficient direction to ensure that Program access to needed information is provided and that the authority to access that information is part of agency policy.

(U) A program may require access to the following information sources:

- **Information Assurance** – system or network audit logs
- **Security** – security violation reports
 - serious incident reports
 - security clearance adjudication files
 - employee financial disclosure reports
 - facility access records
 - foreign travel reports
 - foreign contact reports
 - Statement of Personal History (SF-86)
 - polygraphs reports, if applicable
- **Human Resources** – employee disciplinary records
 - employee employment history
 - job descriptions
 - performance plans
 - employee performance evaluation reports
- **Counterintelligence** – investigative reports
- **IG** – investigative reports
- **Law Enforcement** – serious incident reports
 - investigative reports

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- **External Sources** – External reporting should be identified that may be of significant value, i.e., LexisNexis to cross check information. Exterior information sources can provide alerts not available internal sources.

(U) Records Management Requirements

(U) In implementing a Program, departments and agencies will be required to establish policies and procedures, obtain data from multiple sources, and generate reports and other documents to ensure compliance with E.O. 13587 and the Policy and Standards. The records generated in support of your Program must be managed and preserved in accordance with the guidelines set forth by your agency and the National Archives and Records Administration (NARA).

(U) 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.



(U) Records Retention

(U) Records of all insider threat inquiries should be maintained according to the records retention regulations governing agency information and any system of records that is established to document Program activities. If the agency possesses no clear records retention regulations applicable to insider threat inquiries, the agency records retention professionals should collaborate with the National Archives and Records Administration (NARA) to establish an appropriate system of records and, where appropriate, issue public notification of that system of records. In most cases, however, an agency will already have retention guidelines approved by NARA, perhaps covering files associated with the agency's security activities, counterintelligence activities, or inspector general activities. In any event, the agency's Information Management Office, or its equivalent, should guide the Program personnel in proper records management.

(U) An agency will need to determine: (1) what type of records and/or systems will be created and used in support of its Program; (2) if these records and/or systems should be considered permanent or temporary; and (3) whether the appropriate dispositions are applied to the records and/or systems (i.e., how long these records and/or systems should be maintained) to support the Program. The agency should contact its Information Management Office (IMO) or equivalent to determine if it currently has a NARA-approved Standard Form (SF) 115, *Request for Records Disposition Authority*, or a Records Schedule that supports its Program records. If an approved SF-115(s) or Records Schedule(s) exists to support the program, the Program Manager or designee should work closely with its respective IMO or equivalent in implementing these guidelines to ensure the Program records and/or systems are managed and preserved in accordance with these guidelines.

(U) If an agency does not have an approved SF-115 or a Records Schedule, the Program Manager or designee should coordinate with the respective IMO or equivalent

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

to develop a Records Schedule to support the records and/or systems that will be associated with the agency's Program. Once the Records Schedule is developed, the agency's IMO or equivalent should work closely with NARA to obtain the required approval. Upon approval, the agency's IMO or equivalent should coordinate with the Senior Official or Program Manager (or their designee) to implement these guidelines.

(U) Decisions will have to be made by the agency with respect to the retention period for information and for stored electronic data. The question involves a proper balance of the equities of the Insider Threat Program (i.e., the Program need to possibly refer back to information years after it was originally acquired, even if the information was originally not tied to an insider threat concern), the responsibility to protect the privacy and civil liberties of employees, and the need to follow retention guidelines approved for the agency. Discussions among the agency proponents in each of these areas will be necessary to arrive at a suitable data and information storage plan for insider threat information and data.

(U) Step 5: Seek Legal Input

(U//~~FOUO~~) As the working group proceeds, regularly coordinate each step of the implementation process with General Counsel to ensure compliance with applicable laws and policies. Since Program responsibilities may deal with a significant quantity of personally identifiable information and will involve the individual conduct of employees, great care should be exercised to ensure that the Program provides adequate personal privacy and "whistleblower" protections. All investigative and response manuals and procedures should be coordinated with OGC personnel. Incorporating active counsel and civil liberties membership in the working group should ensure an appropriate level of legal review and guidance for the new Program. (See *Summary of Federal Citations for the National Insider Threat Task Force, page 3.*)



(U) General Counsel

(U) Some agencies have found that a letter or memorandum from The Office of General Counsel outlining the authorities for specific Insider Threat Program functions -- such as the conduct of insider threat conduct and user activity monitoring -- facilitates cooperation and collaboration across the agency with the Program.

(U) Step 6: Protect Privacy and Civil Liberties by Applying Appropriate Safeguards

(U) The E.O.13587 and the Policy and Standards require agency insider threat programs to include appropriate protections for privacy and civil liberties. This includes, but is not limited to, ensuring the protection of the privacy and civil liberties of D/A employees. Information collected, retained, and sharing will likely be subject to the *Privacy Act of 1974* and the *Federal Records Act*. Further, all IC elements will be subject to E.O. 12333 *United States Intelligence Activities*, 4 December 1981; and their Attorney General-approved United States persons guidelines (see *Summary of Federal Citations for the National Insider Threat Task Force, page 3.*)

(U) To assist in this regard, agencies should consult with their civil liberties and privacy officials in developing their agency insider threat implementation plans and policies. These officials should be integrally involved in all working groups established and all activities designed to develop and implement the Program.

(U) The consolidation and sharing of personal information for insider threat programs create privacy and civil liberties risks. Thus, certain minimum procedures are required to safeguard information and people from privacy and civil liberties abuses. These include the following:

- Mandatory training of all insider threat personnel regarding the proper handling of information (and consequences of misuse) and all applicable civil liberties and privacy laws, regulations, and policies governing their activities.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- 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.
- Training of all employees on agency standards, policies, and implementation activities.
- Notification to employees on the monitoring of government systems through written notification and banners on government computer systems.
- Particularized 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 ensuring 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.

(U) Step 7: Identify Classified and Other Critical Assets

(U) Agencies should also consider supplementing these minimum requirements with additional safeguards tailored to their organization(s). If more intrusive insider threat detection measures are deemed necessary by an agency—including as part of any periodical reevaluation or assessment of the agency threat posture—additional safeguards should be adopted to compensate for those measures. Consideration should be given to applying additional safeguards that are, at a minimum, proportional to any increased risks to privacy and civil liberties. These can 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, (see *Information Integration, Analysis, and Response*, page 20) 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 particularized findings and approved by more senior officials.

(U) The E.O. 13587 and the Policy and 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.

(U) Although the Program will apply to clear personnel, the working group should consider whether it wishes to apply its Program to other agency critical assets that are sensitive but unclassified.

(U) 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.

(U) The empanelling of the insider threat working group (see *Step 3: Form Working Group/Periodic Feedback to the Community*, page 5) provides an opportunity to review, across the agency, the maturity of its critical asset risk assessment process.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) There are many risk assessment models that an agency may choose from. One model that looks at an agency from a security and counterintelligence perspective can be found in a small document published by the ONCIX entitled *Counterintelligence/Security Risk Assessment for Federal Partners* and may be found on the NITTF classified website or be requested by contacting the NITTF via e-mail at (b)(3) (classified) or (b)(3) (unclassified).



(U) Drafting Your Insider Threat Policy

(U) While the policy can cover any of the points contained in the White House Memorandum on *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, and this *Guide*, as a minimum it should:

- Establish the Program and direct functional or office managers to support.
- Describe the purpose of the Program (detecting, deterring, mitigating insider threats) in the context of this specific agency's mission.
- Designate the Senior Official(s) responsible for oversight and management of the agency's Program.
- Establish a Program office, including a centralized analysis and response "hub" or center.
- 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, and civil liberties issues are addressed.
- Mandate insider awareness training.
- Establish a user monitoring capability on classified networks and systems.
- Require agency self-assessments of compliance with the Policy and Standards and report results to Steering Committee.
- Enable independent assessments of agency compliance.

(U) Step 8: Write Agency Policy and Implementation Plan

(U//~~FOUO~~) Each agency is required to issue an insider threat policy and implementation plan. Understanding the authorities (see *Step 5: Seek Legal Input*, page 11) under which the Program shall function in the agency, the working group should examine each individual minimum standard in the context of the agency's unique environment. This should aid the group in applying each standard in a way that makes sense, supports the agency mission, and safeguards the agency's classified information. Remember that the agency policy and implementation plan should apply to all agency elements, not solely to the agency headquarters. The *Guide* discusses in detail each individual standard in the next section.

(U) An agency policy will form the framework for implementing the Program. A policy template has been provided that can be tailored to the specific needs of the agency (see *Appendix B*, page 54).

(U) An implementation plan will provide an agency a detailed way forward to establish the Program and a mechanism to advocate for resources, both internally and throughout the executive branch budgeting process. An implementation plan template has been provided (see *Appendix C*, page 59) which can be tailored to the specific needs of the agency.

(U) A comprehensive list of Program functions may be found, in the section entitled "Implementing the Policy and Standards—Responsibilities of the Senior Official(s)" (see page 17). In the implementation plan, the working group should explain how the agency intends to accomplish various agency-specific functions, including:

- Setting timelines and milestones for establishing each element of the Program;
- Explaining Program staffing and resourcing;
- Outlining the responsibilities for a Program Office;

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- Delineates how information from various agency offices will be provided to the insider threat hub;
- Outlining the agency methodology to conduct self-assessments;
- Determining the process through which the agency will respond to agency reporting requirements (including designating the agency office that will be responsible for gathering KISSI information) (see Appendix D for additional information on KISSI, page 65);



(U) Agency Reporting Requirements

(U) The E.O. 13587 and the Policy and Standards establish certain periodic agency reporting requirements:

1. Agency head annual self-assessment report to Senior Information Sharing and Safeguarding Steering Committee
2. Senior Official annual insider threat progress report to agency head
3. Quarterly Key Information Sharing and Safeguarding Indicators (KISSI) report to the Senior Information

- 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; and
- Satisfying agency reporting requirements.

(U) The NITTF is available to assist agencies in developing their Program implementation plans. Any support arrangements should be documented in the plan.

(U) Step 9: Obtain Approval, Establish Program Office, Implement Plan

(U) The working group and the Senior Official should present the agency's 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. At the very minimum, however, agencies should seek to establish a centralized analytic and response capability—a hub—no matter how basic (see *Information Integration, Analysis, and Response*, page 20). 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 supervise implementation of 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 personnel is being assembled, it should be introduced to the entire agency workforce, preferably by the agency head, as part of an agency-wide “roll-out” of the agency'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 agency, which will help meet the requirements of the training and awareness minimum standard (see *Employee Training and Awareness*, page 34).

UNCLASSIFIED//~~FOUO~~

(U) Step 10: Conduct Scheduled Self-assessments

(U) After the agency assigns day-to-day responsibilities for the Program to a Program Office and begins executing the implementation plan, the senior responsible official may want to release the working group. Since, however, the agency policy and implementation plan should have included provisions for periodic Program self-assessments, the Senior Official may wish to confer with the agency head, the General Counsel, and the Inspector General to determine when to assess the agency's progress. The senior leaders may decide to reconvene the working group periodically to conduct an interim assessment of the agency's posture or to assign the assessment function to a separate office, such as the IG.

(U) Remember, the Policy and Standards require two reports, at least annually, on the agency's insider threat posture. First, the senior responsible official is required to provide an annual progress or status report to the agency head on the Program. The Senior Official's report should provide an update on the implementation plan that was previously approved by the agency head, document annual accomplishments, resources allocated, insider threat risks identified, recommendations and goals for Program improvement, and major impediments or challenges. Second, the agency head is required to report annually to the Senior Information Sharing and Safeguarding Steering Committee (established by

E.O. 13587) the results of agency self-assessments of compliance with policies and standards issued pursuant to E.O. 13587. The agency head and Senior Official may want to sequence and structure both of these reporting requirements to satisfy all or part of the agency head's reporting responsibility to the SC. To do this, the Senior Official's annual report should include an internal evaluation or assessment conducted by an agency entity (perhaps the Inspector General) other than the Program Office itself.

(U) In addition to annual reporting requirements, the agency is required to submit responses to KISSI on a quarterly basis. These KISSI results provide the agency with a ready-made information source that should be useful in agency self-assessments. The NITTF recommends that the Senior Official be responsible for, and personally review, the content of each quarterly KISSI submission. The KISSI questions can serve as a good internal measure of an agency's current insider threat mitigation capability. The KISSI questions are constructed to determine compliance with the minimum standards by an agency's Program. As such, analysis of the results of the agency's periodic KISSI reporting to the SC should be a component of the agency self-assessment process. KISSIs can provide the agency with a useful gauge of progress metrics and challenges over time. (See Appendix D for additional information on KISSI, page 65).

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) IMPLEMENTING THE POLICY AND STANDARDS

(U//~~FOUO~~) The Policy and Standards address six major topic areas: designation of a Senior Official; information integration, analysis, and response; Program personnel; access to information; employee training and awareness; and monitoring user activity on networks. Each topic area is discussed below.

(U) Responsibilities of Senior Official(s)

(U//~~FOUO~~) The Policy and Standards require that the agency head designate one or more Senior Official as responsible for the management, accountability, and oversight of the Program. The Policy and Standards list the responsibilities that should be accomplished by that Senior Official(s).

(U//~~FOUO~~) The Policy and Standards envision that, for most agencies, one senior individual shall act as the senior responsible official. However, recognizing that there may be situations where insider threat detection and prevention requires dividing responsibility among several officials (for example, where an agency has multiple agencies or elements subordinate to it and/or distributed over many geographically separated facilities), flexibility is permitted to allow the designation of more than one senior responsible official.

(U//~~FOUO~~) Insider threat detection and prevention require an integrated effort across the entire agency. The Senior Official should facilitate the integration effort, acting as the primary interface between senior leaders across the agency to explain Program requirements and elicit continuing collaboration from the offices led by those senior leaders. In some situations, access to a particularly sensitive information source may need

to be negotiated by the Senior Official. The Senior Official and the agency head should be a visible and positive symbol of the agency's commitment to insider threat detection and prevention.

(U//~~FOUO~~) The E.O. 13587 directs the Senior Official to issue an agency insider threat policy, approved by the agency head, and to develop and promulgate a Program Implementation Plan—both within 180 days of the effective date (21 November 2012) of the Policy and Standards. It is recognized that many agencies were unable to achieve this goal.

(U//~~FOUO~~) In the previous section of the *Guide*, NITTF recommended ten steps the agency and the Senior Official should follow for Program implementation. Among these steps are for the Senior Official to designate an interagency working group (chaired by the Senior Official) and to establish a Program Office. The working group can provide the Senior Official with the initial interagency collaboration necessary to draft the policy and implementation plan and to obtain approval of these documents from the agency head. The Program Office, once approved, resourced, and functioning under the management direction of the Senior Official, should implement the policy and operate the Program. If the Program Office is established at an earlier stage or is assembled within an existing office, then it can contribute to the working group as the latter completes its tasks of writing the policy and developing the Program Implementation Plan.

(U//~~FOUO~~) The Senior Official and Program Office should foster integration of the Program into the operational fabric of the agency by promoting collaboration among stakeholders (see discussion of “stakeholders,” page 7) to actively engage in preventing, detecting, or mitigating insider threat activity. The focus

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

should be on structuring, planning, and overseeing execution of agency insider threat prevention efforts across the agency. A single Program office should centralize agency insider threat knowledge, authorities, and capabilities; address all agency insider threat concerns; and provide insider threat direction, guidance and training, allowing the Program to provide a near-continuous assessment of the strengths and weaknesses of the agency's insider threat efforts. Information should flow from across the agency to a central analytic hub (*see Information Integration, Analysis, and Response, page 20*) in the Program Office. The hub should fuse and analyze the incoming information and initiate an appropriate agency response to investigate or otherwise resolve each insider threat concern. The result should provide an integrated and holistic Program that incorporates participation and information sharing from across the agency.

(U) Note, however, the hub cannot look at everything, so the need exists to constantly refine what "access to information" means. Additionally, the Program Office should consider at establishing automated linkages to facilitate the flow of information and automated analytic tools to facilitate the review of information on a near-real-time basis, if possible.

(U//~~FOUO~~) No matter where the initial organizational work is performed—in a working group or in a new Program Office—the Senior Official must accomplish the same key functions. Each function should be covered in the policy and be described as fully as possible in the implementation plan. This functions include the following:

- Establish a central Program Office to collect and analyze information from all sources to identify insider threat concerns and to initiate appropriate response action.
- 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 agency information about insider threat activities that should be reported to the Program Office, along with reporting mechanisms.
- Employ an insider threat risk assessment capability for the agency, and incorporate the results into the agency's critical asset identification and risk assessments processes.
- Develop agency insider threat awareness training for the workforce per the Policy and Standards.
- Develop a collaborative arrangement whereby advice of counsel is regularly provided to the senior responsible official and the Program Office to ensure that agency insider threat activities stay within legal boundaries.
- Establish appropriate mechanisms to ensure the proper use of information and the adherence to privacy and civil liberties protections within all insider threat activities in concert with the agency General Counsel and civil liberties and privacy officials. (*See Summary of Federal Citations for the National Insider Threat Task Force, page 3.*)
- Leverage information-gathering, analytic, investigative, and operational resources from across the agency 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.
- Provide agency substantive responses to the Steering Committee's quarterly KISSI surveys.
- Establish a system to obtain current U.S. Government reporting on insider threats, trends, and methods.
- Conduct periodic self-assessments of the adequacy of the agency insider threat posture and compliance with E.O. 13587 and the Policy and Standards. The objective should be to conduct periodic reviews of the agency

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Program using expertise external to the Program Office. Two levels of assessment should be considered: effectiveness and efficiency of the agency Program; and compliance of Program Office activities with applicable laws, regulations, and rules. The agency responses to KISSI may be a component of the agency self-assessment process.

- 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. Incorporate analysis of KISSI results, where deemed appropriate. As part of the Program startup effort, progress reports might be warranted on a quarterly basis, perhaps synchronized with KISSI submissions, until the Program is fully established.
- Draft the agency head's annual report to the Senior Information Sharing and Safeguarding Steering Committee, as required by E.O. 13587. Incorporate analysis of KISSI results, where deemed appropriate. The Senior Official's report to the agency head and the agency head's annual report to the Steering Committee may include some of the same information.
- Develop mechanisms to regularly discuss agency insider threat issues with the same agency stakeholders that assisted in the development of the agency's policy and implementation plan.
- Assist the agency mission by contributing insider threat perspectives to decision makers.
- Identify resources necessary to operate an effective and comprehensive Program.
- Regularly collaborate with agency 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 agency 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 as a part of the agency Program. In particular, the FBI can provide invaluable insights to help an agency determine if an insider threat concern warrants referral to the FBI for investigation. In addition, seniors at any of the agencies that have mature programs in place will also be good sources of information and advice.

(U//~~FOUO~~) The Program Office should be staffed with personnel who possess expertise in security, information analysis, information technology, and counterintelligence. Expertise in investigative procedures is also needed, and behavioral science expertise (or behavioral science consultants) may be valuable. To the extent possible, over the course of an individual's professional development training, the Program should seek to cross-train its personnel in more than a single area of expertise.

(U//~~FOUO~~) There is no single "solution" defining where the Program should be located within an agency. The Program may be independent, reporting through the designated Senior Official to the agency head. It can be situated within the agency security office, because insider threat prevention and detection represent one aspect of an agency's security posture, and because a security office will usually be the agency focal point to resolve incidents involving the unauthorized disclosure of classified information. Alternatively, it may be situated within a separate counterintelligence office, which might normally be the agency focal point for handling incidents of suspected espionage. Wherever the Program Office is situated within the agency structure, it should develop and maintain close collaborative ties with the agency Director of Security, Director of Counterintelligence, Chief Information Officer, Inspector General, General

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Counsel, civil liberties and privacy officials, Chief Financial Officer, and Human Capital Resource Officer.

(U//~~FOUO~~) Along with the agency head, the Senior Official(s) should be the primary advocate within the agency for Program resources and overseeing Program resource distribution across the entire agency. The Senior Official should look 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.

(U) Information Integration, Analysis, and Response

(U) Integration

(U//~~FOUO~~) Integration should occur on two levels within the agency. First, it occurs through the outreach and interface by the Senior Official with agency senior leaders who, together, should work to integrate the efforts of individual offices toward successful Program implementation. Second, information from individual offices that “own” discrete pieces of information should be integrated in a centralized office or hub where the information is analyzed, insider threat concerns identified, and response recommendations developed and, where appropriate, pursued to resolve the concern.

(U) Centralized Hub: Information Analysis and Response

(U//~~FOUO~~) Establishment of a centralized insider threat hub should be one of the milestones for Program implementation. The hub should function under the direction of the agency senior insider threat official. The hub has three primary functions: to gather and integrate pieces of information from various offices and sources, to analyze that information to identify indications of possible malicious insider activity, and to ensure that the agency responds appropriately to all insider threat concerns.

- Program and agency leadership should establish procedures to ensure that information is provided to the hub from across the agency and from external sources that are deemed important to the analytic effort. These procedures should be included in the agency Program Implementation Plan.
- Once gathered, the analytic component of the hub integrates that information and analyzes its content to detect patterns of individual conduct that are unusual and that may indicate malicious activity. The analysis of gathered information from multiple sources should create a picture of an individual's activities that would not be available or apparent by reviewing information records or data from only a single source or office.



(U) The Insider Threat “Hub”

(U) The hub is part of an agency's insider threat Program Office. It functions under the direction of the agency senior insider threat official, and is responsible for gathering and analyzing insider threat information, identifying potential insider threat concerns, and ensuring that an appropriate inquiry is conducted to resolve the concern.

(U) For agencies with multiple subordinate elements or numerous facilities spread over a wide geographical area, particular care will have to be exercised to ensure that the hub function is adequate to the breadth of the agency's mission. In these cases, an agency may choose to establish several analytic centers, linked by a central information repository.

(U) An agency with a mature security, counterintelligence, or investigative capabilities may opt to employ those capabilities to perform all or part of its insider threat hub function. In such cases, care will have to be taken to ensure that access to insider threat information is strictly limited to those designated to support insider threat activities and to ensure that the capability is responsive to the direction of the agency senior insider threat official.

(U) These functions may occur in physically separate locations but are coordinated and under centralized oversight.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- Once a possible insider threat concern or anomaly has been identified through analysis, the hub should ensure that further inquiry or investigation is conducted in order to resolve the concern.

(U//~~FOUO~~) Determining what information should flow to the hub should be one of the tasks discussed early on by the agency working group (see *Step 3: Form Working Group/Periodic Feedback to the Community, page 5*) and included in the agency implementation plan. The fact that the working group is composed of agency stakeholders should facilitate the development of procedures to provide hub access to information. Since the stakeholders will understand the content of the various information held by their respective offices, their knowledge should assist the Program Office and hub in identifying which information must flow to the hub.

(U//~~FOUO~~) In some agencies, the information, analysis, and response functions all may be conducted within the hub. In other agencies--particularly those that already have mature security, counterintelligence, or investigative elements in place--senior leadership may opt to have some or all of the hub functions performed by the already-existing elements. However the agency decides to implement its information integration, analysis, and response functions, the conduct of the functions should be overseen by and responsive to the agency Senior Official responsible for insider threat. Implementing arrangements should be included in the agency insider threat implementation plan.

(U//~~FOUO~~) Where already-existing elements are employed to accomplish hub functions, care will have to be exercised to ensure that accessibility to



(U//~~FOUO~~) Five Prerequisites for Implementing a Hub

(U//~~FOUO~~) Prior to analyzing its first item of information, there are five important threshold events that must occur for a central hub to function effectively:

1. Give direction for individual components or offices within an agency to share their information to a central facility as mandated by the Policy and Standards.
2. Identify what agency components are likely to possess information of insider threat interest.
3. Collaborate with each component individually to determine what information within an individual component's holdings would be useful to detect malicious insider activity.
 - 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.
4. Technical Program personnel and the information "owner" should determine how relevant items of

information can efficiently flow to the hub. There are at least two sub-questions that the agency should explore in answering this question:

- Will the information flow to the hub through an electronic pathway or through manual means employing actual human interface with the information? If the latter, define a discreet process for hub personnel to obtain needed information in a timely manner.
 - Does the information lend itself to electronic screening to pull out only items that respond to automated queries or indicators that have been predetermined? If the information lends itself to automated screening, technical expertise will have to be employed to build a suitable electronic screening protocol or mechanism. Agencies may not want to disseminate widely the indicators or triggers developed for insider threat screening purposes.
5. A cross-domain solution should be implemented to restrict access to insider threat activity to only those persons designated by agency leadership as requiring such access. Because of the sensitivity of insider threat information, activities of the Program should not be shared with the general agency workforce.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

insider threat information is restricted to only those persons authorized by the senior official. Arranging appropriate access restrictions will probably require close coordination among senior leaders, particularly between the senior insider threat official and the senior official(s) whose element(s) are to perform insider threat hub functions.

(U//~~FOUO~~) As has been noted, however, the hub will not be able to analyze all incoming data and information. A critical role for the hub will be to define and continually refine indicators on which the hub should concentrate its analysis. Part of this process of definition and refinement should include an understanding of what information resides in the various agency offices and, within each category of information, what content might reasonably be of analytic interest to the hub.

(U) Analysis can be performed manually, through human effort alone, or, ideally, through the combination of human analytic skills and information technology tools. Not everything can or should flow into the hub. With too much information, relevant details may get lost in a volume of data; patterns and anomalies may be obscured by large amounts of information and data. With this in mind, the NITTF strongly suggests that the agency staff its hub with analysts experienced in CI and security. However, even with the best, most experienced analysts, there must be some effort to triage the information flow. To do this, information owners within the agency should meet with the Program Office to define what information is likely to be of importance to the Program. That information should flow to the hub for analysis. Involving the components that own various agency information in setting parameters or guidelines to filter information will reduce the quantity of information flowing to the hub without increasing the risk that critical information points will be overlooked. This task will be difficult but is essential. In fact, the process of defining the information flow to the hub is a form or risk assessment. (See *Access to Information*, page 9 and page 31.)

(U) In some cases, procurement of automated sorting and processing tools can assist the analyst and result in greater insider threat detection than could be achieved through human analysis alone. For the procurement of automated search and analysis tools, the CIO office can be a significant resource in identifying and testing such capabilities. However, even where automation is possible to streamline information access and analysis, the analyst's viewpoint will still be essential in building any automated information triage process in order to determine what is important and what is not.

(U) The agency also will require personnel to conduct investigations. Program investigators, who may also perform the analysis, will pursue anomalies and issues of concern that arise from the hub's analytic efforts. Whether the investigative personnel are actually situated in the hub or some other agency office (such as the agency's CI office, IG office, or Security office), running an issue of concern through to its logical conclusion requires a combination of trained investigative skill coupled with an appreciation for the steps necessary to stay within legal guidelines and to ensure steps are not taken that might compromise any future prosecution.

(U//~~FOUO~~) NITTF would expect that counterintelligence and security files would be potentially rich sources of information for hub analysis. Beyond these sources, there may be several others that a Program should consider for information fusion and analysis. Additional data sources can provide greater fidelity in anomaly detection and resolution as well as produce significant efficiencies, such as quicker resolution times. As Program personnel seek to access each of these information sources, they should work with the agency's General Counsel, and privacy and civil liberties officials, to ensure that Program access to information is always obtained within proper legal and regulatory authority.

(U//~~FOUO~~) As noted previously, the Program should work with its Chief Information Security Officer to automate the flow of information from sources into the hub.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

To accomplish this, it may serve the interests of the agency to have dedicated technical expertise from the CIO office assigned or detailed to the Program Office. Information Assurance (IA) analysts could, for example, participate in the Program's analytic hub adding their expertise to the hub analytic effort. Even if user activity monitoring is not available, IA analysts can assist in providing and interpreting enterprise audit data.

(U) Examples of information sources—some of which may be externally controlled by another agency—that should be accessible to the Program include:

Human Resource files and personnel records—position descriptions; resumes and biographic information; hiring, transfer, retirement, and termination records; promotions and demotions; tardiness complaints; 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.

Chief Information Office and Information Assurance Office files—copier, facsimile machine, and printer usage logs; enterprise audit results; incidents of misuse of U.S. Government computers; and misuse of removable media.

Telephone usage logs—often, an organization keeps call data for billing and policy enforcement. These data usually consist of the phone numbers assigned to the agency, their locations, dates/times of outgoing and incoming calls, and sometimes the external phone number that was connected. These data can often provide additional analytic insight into anomalous conduct.

Inspector General files—results of inquiries as they pertain to individual employees.

General Counsel—leads developed that suggest insider conduct.

External Information Sources—

- **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, pilot, explosives, 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.
- **Intelligence Community (IC)**—information drawn from counterintelligence investigative reports, technical intelligence collection, and human intelligence reports may provide unique insights. Given the sensitivity of the information from these sources, specific sharing arrangements may have to be put in place with each information source.

(U) Trained analysts will be essential to the hub function. The hub will rapidly assemble large quantities of information from multiple offices and sources. Some of the information gathered will not be germane in every case or situation, or will be relevant in a different manner or to a different extent from one case to the next. Combining relevant salary information, travel records, IG, and serious incident reports, criminal allegations, foreign travel records, and performance evaluation report information—among other sources—requires the skill of a person trained in link analysis techniques, trained to find connections where none would otherwise appear to exist. Analysts possess the skill to link disparate pieces of information into a mosaic portraying the activities of each employee. Analysts also have the necessary skills, working in collaboration with individual agency offices, to identify

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

the salient information that should be accessed from among all records maintained by each office.

(U) Response

(U//~~FOUO~~) As integrated information is being analyzed, an insider threat concern may surface. The agency should subject the concern to additional scrutiny through a limited inquiry^b to further clarify the facts and circumstances. The Program Office should determine the agency office entity responsible for conducting the investigation. It may be the sole investigator in the hub or a separate office of trained investigators. That designation should be specified in the agency insider threat policy and within guidelines that detail the investigative procedures and authorities followed in the agency. The agency implementation plan should specify the manner in which insider threat inquiries will be conducted.

(U) As a minimum, agencies possess clear authority under E.O. 10450 to conduct investigative activity to resolve any matter that may suggest whether an individual should be granted initial or continued access to classified information. In addition, some IC agencies may have investigative authorities under E.O. 12333, or associated with specific Attorney General guidelines.

(U//~~FOUO~~) It will be crucial that Program managers and personnel responsible for the actual analysis and reporting process receive thorough training in the conduct and limitations of inquiries. To facilitate such training and to ensure proper oversight, the NITTF recommends that, where possible, Program analytic and investigative personnel should be directed by CI and/or security professionals.

(U) If the inquiry concludes that there is no basis for further action, the investigative report should be labeled as unfounded and no further action taken. A copy of the preliminary inquiry should be filed to document the results of the matter for future reference. Note however, that the agency should establish guidelines for the proper classification of insider threat inquiry information. An *Insider Threat Classification Guide* is currently under development and will be circulated to all agency upon completion. It will also be added as Appendix F to this

Guide. Note also, that the agency should establish retention guidelines for all insider threat-related information, including information pertaining to concerns that are ultimately determined unfounded (see *Records Management Requirements*, page 10).

(U) An agency investigative response should be centrally managed in order to oversee the quality of the effort. Central management will ensure that all investigative activities remain within the bounds of legal and regulatory authorities. Central management will also help provide for proper training of investigative personnel, and ensure that investigative activity is accurately documented for accountability and future reference.

(U) In larger agencies with several subordinate entities, central management may require investigative management at multiple locations. In all cases, however, the agency should seek to have an investigation managed by a single office. If such an arrangement is not possible, great care will have to be taken to ensure continuity of effort, protection of the evidentiary chain, and protection of privacy and civil liberties of all individuals. Protecting employee reputations is paramount.

(U//~~FOUO~~) If the inquiry reveals that there is a basis for a more formal review or investigation, the results of the inquiry become the first step in a more wide-ranging response. Most likely, the appropriate response will be to refer the body of the inquiry to a law enforcement or CI investigative authority with jurisdiction to conduct a more comprehensive investigation of the concern. Exactly when a preliminary insider threat inquiry reaches the point of maturity or concern that it should be referred to another entity—including to an outside investigative agency such as the FBI—differs in each case. As a result, close coordination between the Program and the agency General Counsel will be essential to determine if and when the Program should enlist the help of another authority.

(U//~~FOUO~~) The Policy and Standards emphasize the importance of integrating counterintelligence, security, information assurance, and human resources information to identify potential malicious insiders. The Program

^b Note: For the purposes of response actions, this *Guide* uses the terms “investigation”, “inquiry”, and “assessment” interchangeably.

UNCLASSIFIED//~~FOUO~~

personnel should be mindful that, while protection of classified information and the ability to mitigate the damage that a malicious insider can do are principal reasons for implementing insider threat programs, the same information may serve as the predicate for an espionage investigation by CI authorities.

Counsel should minimize the possibility that preliminary investigative activity would taint any subsequent counterintelligence inquiry or that visible actions would alert a potential insider.



(U) 811 Referrals

(U) *Section 811c, Intelligence Authorization Act for Fiscal Year 1995*

(U) "The head of each department and agency within the executive branch shall ensure that . . . the [FBI] is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power . . .

(U) "The Director of the [FBI] shall ensure that espionage information obtained by the [FBI] pertaining to the personnel, operations, or information of departments or agencies of the executive branch, is provided through appropriate channels to the department or agency concerned and that such departments or agencies are consulted with respect to espionage investigations undertaken by the [FBI] which involve the personnel, operations, or information of such department or agency."

(U)(b)(7)(E) [Redacted]

(U//~~FOUO~~) The agency must have internal procedures to guide the conduct of the insider threat inquiry. Those procedures should spell out how response actions will be coordinated with the Office of the General Counsel. Such coordination should ensure that inquiries are conducted within proper limits, should ensure that the individual's privacy and civil liberties are protected, and that the inquiry does not taint evidence or jeopardize a possible investigation or prosecution by a law enforcement agency. (See *Summary of Federal Citations for the National Insider Threat Task Force*, page 3.)

(U//~~FOUO~~) Program personnel should receive training on how and to whom to make referrals. For example, Program personnel must be 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.) Likewise, should the matter indicate that a referral to the Security Office, Inspector General, or a law enforcement agency is warranted, policy and procedures should be in place to ensure that the referral is made in a timely and efficient manner.

(U//~~FOUO~~) The ability of the CI element to investigate and successfully gather evidence that is admissible at trial may hinge on the manner in which the insider threat inquiry is conducted. In other words, while the goal of the insider threat inquiry is to gather enough information to form the basis for a response to the insider threat concern, that inquiry must not prejudice any future investigative prerogatives that fall under the purview of the CI element. Once again, close coordination between the Program personnel and the agency General

(U//~~FOUO~~) If the matter becomes an espionage investigation, the status of the subject under investigation (military, civilian) and the location of the alleged offense (in the United States or overseas) will have a direct bearing on which CI element has primary investigative jurisdiction. Again, the coordination with OGC will assist with such determination.

UNCLASSIFIED//~~FOUO~~

(U) Additional guidance on the proper conduct of inquiries and investigations can be found under the section dealing with Program Personnel (see, page 27)^c.

(U//~~FOUO~~) Following referral of a concern to an administrative or investigative entity, the agency should continue to monitor the status of the referral to ensure that the agency receives timely feedback on the outcome. Through feedback, the agency can determine if other actions, in coordination with the investigative entity, should be taken. Knowing the final disposition of the matter also provides valuable information that can aid in process and program improvements and in the ongoing training of insider threat detection personnel.

(U) In addition to training Program Personnel in 811 Referrals, the response function of a Program Office can be strengthened by using the 811 Referral process as a means to establish a substantive working association with the FBI. Not only will this help ensure that referrals are made to the FBI in a timely manner, it will also open a dialogue between the agency and the FBI that can yield FBI insights on potential matters of insider threat concern. In this way, the FBI can serve as a valuable resource to assist the Program Office in deciding its response options and, when necessary, guide agency inquiries and investigations in a way that ensures, to the maximum extent possible, that the



admissibility as evidence of any agency-developed information is preserved in the event that the matter reaches the level of a legal prosecution.

(U) An 811 Referral sample is provided at Appendix E (see page 68). Note also that counterintelligence or counterterrorism matters may also be of interest to the FBI and should be reported, even if they do not meet the 811 reporting criteria close working relationship with the FBI should facilitate these matters.

(U) Access to Behavioral Science Services

(U//~~FOUO~~) Behavioral science subject matter experts study human behavior and the social and cultural context in which the behavior occurs. Behavioral Science can identify conduct of concern, contribute to analysis within the hub, and support inquiries and investigations into insider threat concerns. Current mature Programs use behavioral science subject matter experts (SMEs) for a broad range of tasks to support the mission to deter, detect, and mitigate the insider threat. The NITTF recommends that agencies incorporate behavioral science expertise as part of their Program personnel. The agency may obtain, either through internal resources or via external agreement, national security psychologist expertise for insider threat consultation.

(U//~~FOUO~~) When embedded and fully integrated in a Program, behavioral science SMEs bring a unique perspective and a balanced view of the “whole person,” to the Program mission. The whole person approach takes into consideration as much information as possible, including a person’s psychological and physical state, as well as the individual’s social, cultural, and physical environments. Behavioral science SMEs provide objective, unbiased assessments and recommendations based on the analysis and integration of many different types of information. They are skilled at identifying and analyzing suspicious patterns of conduct and insider threat indicators on many levels. They can help evaluate training and reporting relating to an individual’s anomalous conduct.

^c Note: NITTF is developing a procedural manual to assist agency in the conduct of inquiries.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U//~~FOUO~~) The activities, methods, techniques, and tools used by a behavioral science SME vary depending on the specific mission of the department or agency in which they are embedded. Regardless of mission, the primary role of behavioral science SMEs within a Program is to support the team via consultation, research, and training and awareness. Programs make decisions with significant impact, based on the assessment of employees' conduct, so having a trained and experienced behavioral science SME on the team can provide additional validity and credibility to those decisions.

(U) Additional information on the employment of Behavioral Science expertise may found on the NITTF classified web portal, (b)(3) [REDACTED]. The University of Nebraska's ***Behavioral Science Guidelines for Assessing Insider Threats***, which was published in 2008 for the DoD, can be requested by contacting the NITTF via e-mail at (b)(3) [REDACTED] (classified) or (b)(3) [REDACTED] (unclassified).

(U) Insider Threat Program Personnel

(U) Program personnel will have access to user activity information that could be career-damaging or highly embarrassing. With this in mind, the agency should establish limits for the official use, retention, and safeguarding of personal information by Program personnel. Program personnel should receive periodic training in the proper use, retention, and safeguarding of this and all insider threat-related information that they receive. The vast majority of insider leads do not pan out, reinforcing the need for information to be used discreetly.

(U//~~FOUO~~) The amount of personal information that will flow to Program personnel stems from the fact that the Program Office, once established, will serve as the agency's integration and analysis hub. It will be to that hub that information will flow from offices across the agency as well as from sources external to the agency. Therefore, to ensure proper use of this information

Program personnel must understand security, and counterintelligence principles, techniques, and tools. Most of these security and CI capabilities will be employed to analyze information and to investigate and resolve insider threat concerns that surface through the analysis of the information that is received in the hub.

(U) The agency should ensure that the Program Office, the Office of the General Counsel, and the agency civil liberties and privacy officials establish strong collaborative relationships to ensure that Program personnel become intimately familiar with the laws and regulations governing privacy, use, and protection of personal information, and the civil rights and civil liberties of individual employees. The Program Office should consult with agency counsel and the privacy/civil liberties professionals during insider threat investigations. The Program personnel should receive training to understand the important contributions legal, privacy, and civil liberties advisors make to the Program.

(U) Program personnel also must understand the parameters of their agency's authority to conduct inquiries or investigations. Agencies must be able to answer the question: What authority does the agency have to conduct insider threat investigations and in what agency office(s) is that authority vested? In some agencies, 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. In all cases, however, an agency does have the authority and responsibility to investigate concerns that arise with respect to the safeguarding of classified information within the agency. The limits of that authority, however, are matters on which agency legal counsel must advise. (See *Summary of Federal Citations for the National Insider Threat Task Force*, page 3.)

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) Garrity Warning

- (U) An advisement of rights usually administered to federal employees and contractors in internal investigations.
- (U) Advises interviewees of their criminal and administrative liability for any statements they may make.
- (U) Advises interviewees of their right to remain silent on any issues that tend to implicate them in a crime.
- (U) Promulgated by U.S. Supreme Court in *Garrity v. New Jersey* 35 U.S. 493 (1967).
- (U) Helps preserve the evidentiary value of statements provided by individuals during internal administrative inquiries, should the matter also result in criminal investigation.

- (U) 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."

(U) General Counsel and the agency's civil liberties and privacy office should advise the agency and the Program Office regularly on limits that may exist to the agency's investigative authority, the boundaries within which an agency inquiry or investigation can be conducted, and the proper collaborative relationship that should exist between the agency and an external law enforcement entity, such as the FBI. A thorough understanding of investigative limits should be included as part of the regular training for Program personnel. Such training—perhaps taught by General Counsel and privacy/civil liberties representatives—should emphasize how to provide proper privacy and civil

liberties protection to individual employees. The training should ensure that an agency 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. **Insider inquiries must not be used for political purposes, obstructing first amendment rights, or retaliating against whistleblowers.**

(U) General Counsel should provide Program personnel with appropriate advice and guidelines to determine when information received meets criteria requiring referral of the information to other investigative agencies. For example, DoD has established rules requiring that, once a threshold of information has been attained, certain types of investigative actions be referred by DoD agencies to specific DoD entities for all further investigative activity. Some large civilian agencies, with multiple subordinate components, likewise may 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).

(U) Another area in which agency counsel can provide important assistance is in guiding agency insider threat activities—particularly investigations of employees for anomalous activities—through the evidentiary considerations that surfaced in the *Garrity v. New Jersey* law case. This 1967 Supreme Court case established a rule prohibiting the introduction of self-incriminating evidence into federal criminal prosecutions if it appears that the evidence was obtained from a defendant under threat, or perceived threat, that the defendant would lose his or her job for failing to provide the evidence. An agency conducting an inquiry or investigation into an insider threat concern will probably not know at that time that a criminal prosecution will result. However, if the agency's investigative actions present a coercive appearance, then a court may prohibit the use of those investigative results as evidence in a subsequent criminal trial. To the maximum extent possible, an agency will want to conduct its insider threat activities in a manner that will

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

preserve the ability of law enforcement officials to use the information from those activities as legal evidence in any future prosecution. This becomes a judgment call as agencies cannot avoid all interviews. As close advisors to the Program, agency counsel and the FBI can advise on Garrity concerns and assist in preserving the evidentiary integrity of all information gathered through the agency's internal investigative actions.

(U) Program personnel should:

- Safeguard investigative information, to include appropriate limitations on access and use;
- Be trained on all applicable laws and policies and the consequences of misuse of information for personal or other unauthorized purposes;
- Sign nondisclosure agreements and an acknowledgment of governing policies and standard operating procedures;
- Be recused from any activities conducted due to personal relationships with persons under review or investigation; and
- Have significant experience and skill in the following areas: Security, Counterintelligence, Information Assurance/Cyber Security.

(U) **Security Skills**—The following represent skill competencies that should be considered for persons who are brought into the Program Office to provide security technical expertise:

- Professional tradecraft skills associated with security skills:
 - Elicitation
 - Evidence gathering
 - Information security
 - Management and compliance
 - Observation
 - Researching
 - Security program management

- Tools and methods
- Subject matter expertise:
 - Academic/professional disciplines
 - Certification and Accreditation process
 - Classification management
 - Communications security
 - Continuity of operations planning/mission assurance
 - Counterintelligence
 - Counterproliferation
 - Counterterrorism
 - Cultural expertise
 - Incident response
 - Information assurance/cyber security
 - Intelligence disciplines (SIGINT, HUMINT, IMINT, etc.)
 - Investigations
 - Languages
 - Law enforcement
 - Operations security
 - Personnel security
 - Physical security
 - Polygraph
 - Protective services
 - Security education and training
 - Vulnerabilities assessment and management

(U) Note, this skill list was extracted from ODNI's ICS 610-13, *Competency Directory for Security*, October 2010. This document contains skill descriptions and can be requested by contacting the NITTF via e-mail at (b)(3) (classified) or (b)(3) (unclassified).

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) **Counterintelligence**—The following represent skill competencies that should be considered for persons who are brought into the Program Office to provide counterintelligence technical expertise. For ease of discussion, the skills are subdivided into those that apply to CI investigators and those that apply to CI analysts, though they all are often commonly found in experts from both areas:

- CI analytic skills:
 - Knowledge of intelligence collection systems and operations
 - Knowledge of organizational culture
 - Ability to analyze information
 - Information ordering ability
 - Knowledge of CI operational techniques and perspectives
 - Information gathering and assessing
 - Pattern recognition
 - Analytic tools and methods
 - Knowledge of interrelationships among organizations
 - Knowledge of home organization's operations and requirements
 - Knowledge of adversary or target
- CI investigative skills:
 - Knowledge of applicable laws, regulations, policies, and organizational procedures
 - Knowledge of various cultures and adversary modus operandi
 - Investigative expertise
 - Ability to relate and interact with others
 - Communication and presenting information
 - Information-gathering for investigations/inquiries

- Written communication
- Ability to Interview and elicitation information
- Ability to analyze information
- Problem solving and decisionmaking
- Ability to organizing, planning, coordinating work
- Vulnerability assessment

(U) Note, this skill list was extracted from ONCIX's *Fundamental Elements of the Counterintelligence Discipline, Technical Competencies for Counterintelligence Functions Volume 2*,^d August 2007. This document contains skill descriptions and can be requested by contacting the NITTF via e-mail at (b)(3)

(b)(3) (classified) or (b)(3)

(unclassified). Additionally, the ODNI is preparing a directory of counterintelligence competencies, which will replace the August 2007 ONCIX document.

(U) **Information Assurance/Cyber Security**—The following represent information assurance skill competencies that should be considered for persons who are assigned to the Program Office for the purpose of establishing and managing the organization's user monitoring capability and automated information processes:

- Experience as Information System Security Officer or Manager (ISSO/ISSM), information security, information assurance (security architecture and applications security), systems engineering, computer engineering, network engineering, or program management
- Possesses a Certified Information System Security Professional (CISSP) certification
- Understands Public Key Infrastructure (PKI) and access security
- Understands how to obtain artifacts needed to conduct a security control assessment (e.g., policies, procedures, plans, specifications,

^dThis is classified document.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

designs, records, administrator/operator manuals, information system documentation, interconnection agreements)

- Understands various user monitoring technical tools
- Understands how to obtain and employ the results of the organization's system audit capabilities for insider threat analysis
- Understands the difference between an organization's system audit capabilities and user monitoring capabilities
- Has the ability to analyze technical threats and challenges related to insider threat programs
- Understands applicable laws, regulations, policies, and organizational procedures governing information assurance and insider threat
- Understands information technology to include computing design concepts and implementation
- Has the ability to assess technical characteristics of cutting-edge developments
- Understands of the organization's diverse information technology infrastructure, including operating systems, major application systems, and network architecture
- Understands the data transfer responsibilities
- Understands counterintelligence and the Internet/CI implications of technology

(U) Note, this skill list was extracted from ONDI's ICS 610-9, *Competency Directory for Information Technology (Mission and Enterprise)*, amended 4 October 2010; and DoD's Department of Defense Manual 8570.1-M, *Information Assurance Workforce Improvement Program*, Change 3, January 2012. These documents contain skill descriptions and can be requested by contacting the NITTF via e-mail at (b)(3) (classified) or (b)(3) (unclassified).

(U) Access to Information

(U) For the Program to succeed, it should have continuing access to information "owned" or maintained by other offices within the agency. Several information source types—human resources files, information assurance alerts and logs, security records, and counterintelligence information—are identified in the Policy and Standards as important to the Program. There are other information sources that are not mentioned in the Policy and Standards that may be equally important—for example, Inspector General files, serious incident reports, law enforcement reports, and LexisNexis-type service feeds. The source of information is particularly sensitive therefore procedures should be established by which the Program can obtain access to that information for Program purposes.

(U//~~FOUO~~) One may not always know what type of information may be needed by insider threat personnel to resolve a concern. Some concerns may involve extremely sensitive information, such as information held in a compartmented program or in the personal file of an executive. In such cases, the Senior Official should define the rules of access by Program personnel to ensure security and need-to-know are respected.

(U) As collaboration develops between the Program Office and other offices across the agency, it will become possible to identify, in advance, categories of information of insider threat interest. Identifying such categories as soon as possible should permit controls to be put in place to facilitate a near-automatic flow of such information to the Program's central analytic hub. As mentioned earlier, the agency should attempt to automate access to this information if feasible and effective.

(U) There also may be records of agencies where an employee previously sought employment. These are not generally shared, one agency to another, and obtaining access to other agency information may prove challenging; however, the Program should attempt to establish interagency agreements to

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

permit an exchange of information for insider threat analytic purposes on employees who were previously considered for employment by another agency.

(U//~~FOUO~~) Foreign Travel and Foreign Contact Reporting

(U//~~FOUO~~) These are necessary elements of an insider threat detection program. Research shows that unauthorized travel outside the United States and close and continuing contact with foreign nationals have often been factors in espionage cases. Thus, anomalous foreign travel and contact with foreign nationals have emerged as indicators of potential insider threat activity. As a result, it is incumbent upon agencies to require this reporting, perhaps as part of a larger, comprehensive agency security program. The Program should have access to this reporting and review it regularly for conduct that might be indicative of inappropriate insider threat activities.

(U) Agencies should:

(U//~~FOUO~~) Require cleared personnel to report close and continuing contact with foreign nationals and report both personal and official foreign travel to an appropriate agency office. The information reported should be accessible to the Program. As soon as practicable, the agency should establish an automated capability through which cleared personnel can report foreign travel and foreign contacts. The automated system should be searchable and contain the following information:

- Full name
- Clearance level
- Travel destination
- Designation of travel (as either official or personal)
- Dates of foreign travel
- Travel companions
- Name and nationality of foreign contact
- Location of foreign contact
- Date(s) of foreign contact



(U//~~FOUO~~) Unreported Foreign Activities

(U//~~FOUO~~) The following is an expanded list of unreported activities that should be of concern to the insider threat program:

- Unreported personal contacts with:
 - Known or suspected foreign intelligence services
 - Foreign governments or organizations
 - Unauthorized persons seeking classified information
- Unreported close and continuing contact with foreign nationals, including intimate encounters, sharing living quarters, or marriage
- Unreported actual or suspected approaches by foreign intelligence and security services or non-state actors
- Unreported relatives, associates, or persons sharing living quarters connected with:
 - Foreign governments
 - Foreign intelligence services
 - Criminal or terrorist activities
 - Disloyalty toward the United States
- Unreported foreign travel, defined as any unreported personal foreign travel or unreported or unusual changes in itinerary during official foreign travel

(U//~~FOUO~~) The agency should mount a campaign to make all cleared employees aware of their responsibilities to report foreign travel and foreign contact. This awareness initiative should include clear instructions on how to report and whom within the agency to approach with questions or issues. If feasible, security and counterintelligence officials in the agency should provide threat awareness information to cleared employees prior to traveling overseas and should conduct post-travel debriefings to ascertain any threats encountered during the travel. If individual briefings and debriefings are not possible, an information packet and/or questionnaire

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

can be provided to the traveler, both before and after travel. Though personal interface with the traveler is preferred, an information packet and questionnaire can still elicit valuable information and alert the traveler to the dangers associated with foreign travel.

(U//~~FOUO~~) As the agency automates its flow of information into the central hub, it should include a provision for a centralized application for employees to enter foreign travel and foreign contact information. An automated reporting process can aid in the detection of foreign travel or contact that goes unreported by the cleared employee. Unreported foreign travel and foreign contact can be significant insider threat indicators because they suggest a desire to conceal conduct, circumvent counterintelligence and security protocols, and, perhaps, mask espionage tradecraft.

(U//~~FOUO~~) Personnel Information Retained by Human Resources Offices

(U//~~FOUO~~) 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 can provide the insight needed to make timely and effective decisions concerning disposition and future actions required to resolve an anomaly or mitigate potential risk. For example, there is some evidence from the private sector that an organization is at the greatest risk for theft of controlled or sensitive data by an individual within 30 days prior to an employee's employment termination.

(U//~~FOUO~~) There are laws and regulations that govern the collection, retention, and sharing of HR personnel information. An effective Program will, in collaboration with its General Counsel, become conversant with these rules and will establish a healthy working partnership with HR to ensure that information is shared, used, handled, stored, and protected in accordance with those laws and regulations.

(U//~~FOUO~~) Beyond the basic biographic information available through HR, that office can provide additional information of value to the Program, including job assignments, performance reviews, 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.

(U//~~FOUO~~) Information Assurance and Information Technology

(U//~~FOUO~~) The Information Assurance and Information Technology components of the agency—often situated within the Office of the Chief Information Officer (CIO)—collect network information, system logs, and audit data that can be relevant to an effective Program. The Program should establish procedures to ensure that data flow to the centralized hub and Program personnel include technically trained persons with the skills to translate the data into useful information.

(U) Since both the CIO and the Program both deal in activities and anomalies that occur on networks and systems, confusion may arise between CIO experts seeking to maintain system integrity and availability and Program personnel concerned with user activity on those systems. This is one area where prompt action and guidance by senior agency leadership can resolve a problem before it materializes and can also lay the foundation for what should be mutually beneficial collaboration in the future.

(U) Particularly when fused and analyzed with data and information from other sources, network and system data can provide missing context for user conduct as well as identify potential anomalies. Additionally,



(U) Frequency of Meetings

(U) Meetings between the IA program and the insider threat Program should occur on a regular basis to compare anomalies as well as to discuss newly-identified patterns of concern or the successful resolution of previous patterns for users and computer systems.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

collaboration with the CIO will be necessary for the Program to install its user activity monitoring capability within agency-owned systems. Likewise, the CIO may have unique contacts with external system service providers—that is, organizations outside the agency that own classified networks and permit the agency to access to those networks under rules set by the providing organization. The DoD is an example of a service provider. DoD owns the secret-level SIPRNet and provides agencies access based on rules usually set forth in a memorandum of agreement or service level agreement. Since many agencies draw all or most of their classified systems support from external service providers, the Program can build on those relationships to establish its insider threat user monitoring capability for externally owned systems (see *Established User Activity Monitoring Capability, page 41*). CIO collaboration with those providers can assist. Also, while the agency will want to limit access to the user monitoring results to only those within the Program, collaboration with the CIO may provide to the Program a degree of technical expertise that might otherwise not be available to the Program. It may also serve the interests of the agency to have dedicated technical expertise from the CIO office assigned or detailed to the Program Office. IA analysts could, for example, participate in the Program's hub.

(U) Employee Training and Awareness

(U//~~FOUO~~) A highly trained and aware workforce is key to the early detection 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.

(U//~~FOUO~~) It is important to invest time and resources to educate the workforce, systematically and repeatedly, on the risks associated with insider threats. This includes training on how to recognize and appropriately report basic threat conducts. Proper

training of the workforce will be a necessary element in overcoming the “failures to report” described in the preceding paragraph. Furthermore, training drives home the message that vigilance is necessary because of the enormous damage that can be caused by malicious insiders. One has only to look at the over 700,000 sensitive and classified documents released to the public through the 2010 WikiLeaks disclosures to realize the damaging effects 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.

(U//~~FOUO~~) Programs should maintain an employee awareness and training campaign, focusing on insider threat for all personnel, but particularly for cleared personnel. If possible, awareness training should not be restricted solely to employees with security clearances. While not everyone will have access to classified information and systems, everyone can be aware of and report anomalous or unusual conduct in the workplace. The campaign should start with entry-on-duty orientation for new employees and, as a minimum, include awareness education annually thereafter. The campaign can be conducted in person or via computer-based training and, in addition to the specific requirements set forth in the Policy and Standards, might also include the following:

- Importance of reporting—don't assume a concern is unimportant
- Insider threat indicators
- Methodology of foreign intelligence services or terrorist organizations to target and elicit information from cleared personnel
- Procedures for reporting suspected insider threat activities
- Foreign travel reporting requirements
- Foreign contact reporting requirements
- Financial disclosure reporting requirements
- User activity monitoring

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U//~~FOUO~~) Care should be exercised to familiarize employees with agency procedures for reporting suspicious or anomalous activity to the Program Office, security office, counterintelligence office or other centrally designated location appropriate to the agency. Consider creating an electronic reporting system for all employees.

(U//~~FOUO~~) Insider threat awareness program training can consist of one individual course module that incorporates the key topic areas or can be addressed through several separate training modules. Often, such modules are already in place in other agencies and may be available for the asking. However, an agency should ensure that training borrowed from other agencies is properly tailored and focused on insider threat and the unique environment and mission of the employees receiving the training.

(U//~~FOUO~~) A record should be maintained of all employees who receive—and who do NOT receive—insider threat awareness training. This will permit follow-up action by the Senior Official with those agency offices where participation appears weak, as well as permitting the Program Office to highlight individuals who have yet to receive awareness training.

(U//~~FOUO~~) In providing awareness training, an agency should solicit feedback regularly from audiences and maintain metrics to gauge the effectiveness of the training. Among the metrics that an agency might select would be the percentage of personnel required to receive training that actually undergo the training; numbers of incident reports received by the Program Office within a short period—perhaps 30 days—of the completion of a training event; and recorded comments from audiences using feedback forms.

(U) Additional guidance on building an insider threat training and awareness campaigns can be found in the *U.S. Government Insider Threat Detection Guide, 2011* which is a classified document written by the National Insider Threat Working Group and published by the ONCIX, and can be requested by contacting the NITTF via e-mail at (b)(3) (classified) or (b)(3) (unclassified).

Also, ONCIX and the FBI produced an excellent training video titled “Betrayed” which is available at their websites for downloading.

(U//~~FOUO~~) Implementing a Host-Based User Activity Monitoring (UAM) Capability

(U) Introduction

(U) How an agency establishes a UAM capability will depend largely on whether the agency owns and operates its own system or subscribes to another system owned and operated by another agency. This fact should be determined before any other UAM work is considered.

(U) Overview

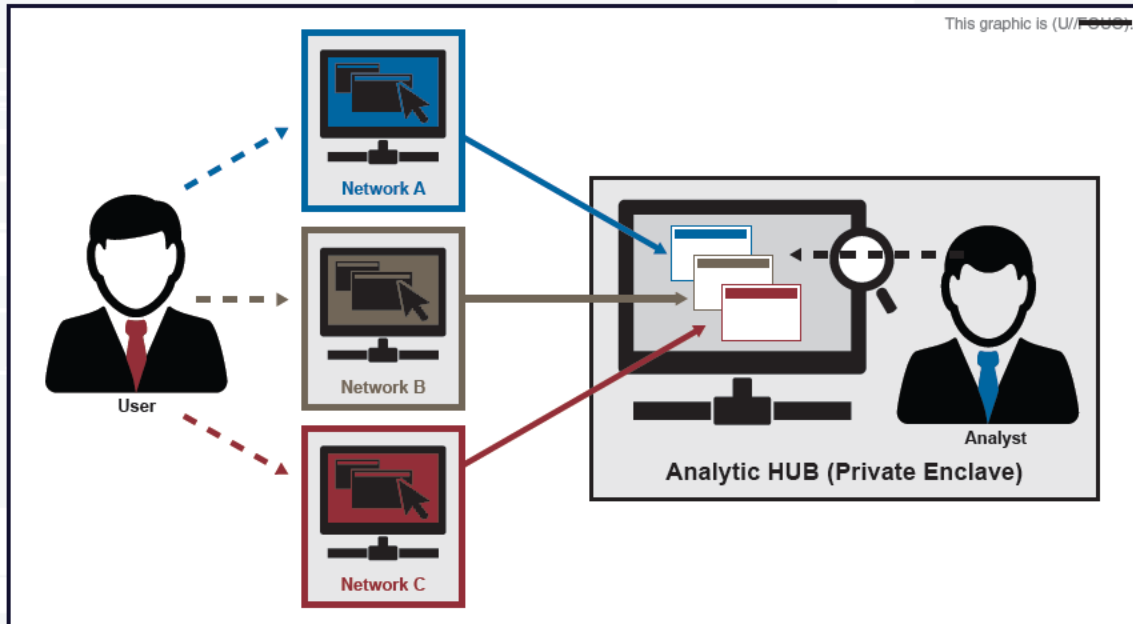
(U) This chapter of *The Guide* assists agencies that are starting the initial implementation of a host-based solution for computer user activity monitoring. The *Guide* first defines UAM and contrasts it with enterprise audit. Second, it provides some necessary background about UAM. Third and finally, it recommends nine steps to implement a host-based software solution, as required by the Policy and Standards.

(U//~~FOUO~~) A UAM solution helps the Program with the following:

- Collecting highly detailed computer user activity data and send it to the hub as an information source for inclusion in the hub’s analytical process to detect insider threats
- Allowing near-real-time review of computer user activities on a host computer to assist in inquiries
- Providing clear, non-refutable evidence of specific user actions on his/her host computer
- Providing storage for the collected data

(U) Figure 2 (see page 36) shows how a UAM program could operate across multiple security domains and networks to consolidate the data at the highest classified network in the hub.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~(U//~~FOUO~~) Figure 2: User Activity Monitoring (UAM)

(U//~~FOUO~~) UAM is performed on all classified networks and sends the collected data to the hub for in-depth monitoring and analysis.

(U) UAM Defined

(U) UAM refers to 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 should have the minimum capability to observe and record:

- Key strokes
- Content of chat
- Content of files and documents
- Screen capture of display
- Video capture of display activities
- Capture of file versions as they are edited
- Web browser activity
- Clipboard (copy, cut, and paste) activity
- Files accessed

- Kernel processes
- Applications executed by user
- USB port activity
- Removable media activity
- E-mail content

(U) UAM data should be available for analysis and processing in near real-time. The product of UAM will be in the format of text descriptions, screen captures, and full-screen video capture.

(U) Analysis of these various data elements provides information about the activities of the user on a particular computer.

(U) UAM applies software logic while collecting the data to identify computer activity that is of insider threat interest or concern. This software logic is sometimes referred to as alerts, policies, algorithms, or triggers. For purposes of consistency, the *Guide* uses the term “logic” to represent these terms.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) The collecting and storing of user activity data should be done in accordance with all applicable laws and policies to avoid conflict with privacy and civil liberty laws. The parameters within which UAM will be conducted should be developed in collaboration with OGC and incorporated into the insider threat implementation plan to be submitted to the agency ahead for approval.

(U) UAM data may include classified information. Classification of UAM data will be equal to the highest classification from which the data was obtained.

(U) UAM Using Host-Based Software

(U) Host-based UAM software can collect all or some of a computer user's activity on the host computer, including keystrokes, and screen capture (still and full-motion video). UAM is necessary because all of the details of a user's activities on a host computer cannot be collected elsewhere by other means. Examples of actions of interest would be a user typing specific sensitive keywords into the computer, copying or cutting text from a document, and executing any search on the local computer, network drive, or website. Effective UAM would collect the details of each of these activities for analysis to detect questionable conduct.

(U) A method of Host-based UAM capabilities must be implemented. Any host-based UAM capabilities should communicate with a server and database, providing configuration information, licensing, and data storage capabilities.

(U) There are several commercial-off-the-shelf UAM software packages available for an agency to consider. The NITTF can assist the agency in obtaining information about these various vendors. NITTF also can assist by introducing agencies to other U.S. Government agencies that have experience individual vendor products and capabilities.

(U) Enterprise Audit is NOT User Activity Monitoring

(U) Enterprise audit (EA) is an independent review and collection of records and activities, employed by the Chief Information Officer of an agency, to assess the adequacy of system controls on computer systems operated by that agency and to ensure compliance with established policies and operational procedures. EA involves the identification, gathering, correlation, analysis, storage, and reporting of information about the system. EA usually will employ the use of records—called audit log files—that chronologically record the activities that occur on a system, including records of system accesses and operations performed in a given period.

(U) EA information is one of several data sources used in insider threat detection. However, many activities performed by an individual on his/her computer will not be detected or collected using EA. It will not gather the substantive content of the user's computer activity, an important information source for insider threat detection. For that, a host-based UAM capability is required.

(U) Safeguarding and Protecting UAM data

(U) UAM activities and data are highly sensitive for the following reasons:

- **Privacy Information**—UAM data may contain private information such as social security numbers and passwords;
- **Potential to Damage an Individual's Reputation**—The fact that an individual is being monitored for insider threat conduct is sensitive information. If divulged, it could impact a user's career or an ongoing investigation; and
- **Alert Malfeasance**—UAM tactics, techniques and procedures, if generally known, would permit insiders to change their tradecraft or computer activity to avoid detection.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) It is important to limit access to the UAM data. Because of the sensitivity of the information, the UAM solution should be hosted in a separate private enclave, which would be accessible only by Program personnel and have very limited connectivity to systems outside the network. This approach will safeguard the UAM data by limiting access while protecting the operational network from analytic activity within the private enclave.

(U) UAM data must move from the agency production or operational network environments to the private enclave. Network connections into the UAM private enclave should be protected using automated, trusted one-way transfers (a cross-domain solution). The routing of the data across the network is a technical issue that will be the responsibility of the Program staff or service provider in collaboration with the CIO, as appropriate.

(U) Importance of Coordination and Communication with CIO

(U) A significant lesson learned from several of the departments and agencies with established insider threat programs and UAM capabilities is to develop a close and open working relationship with the CIO, which will be mutually beneficial to both offices. The Program Office will benefit by receiving valuable guidance about the current environment, future plans, technical challenges and solutions. The CIO can benefit by having a complete understanding of the Program plans, challenges, policies and issues; however, in order to limit exposure of the UAM software logic outside the Program, the CIO's knowledge of the UAM capability should not include access to the software logic and collection details.

(U) The CIO should be responsible for the following activities:

- Deploying the host-based software (based on department and agency policy);
- Deploying regular configuration updates;
- Reviewing performance test reports of the impact of the host-based software on computers and networks;

- Supporting Program activities to monitor the deployment and use of the host-based software; and
- Supporting the routing of UAM data across the network into the analytic hub.

(U) The CIO normally should NOT be involved in the following insider threat Program activities:

- Defining, developing, and testing the UAM software logic;
- Storing and retaining the UAM data; and
- Reviewing and analyzing UAM data.

(U//~~FOUO~~) Administrative access by the CIO staff to Insider Threat Program equipment and software should be limited to the fullest extent possible.

(U) Note, initially in some smaller agencies, it may be necessary for CIO personnel to participate in these activities. If this becomes necessary, great care must be taken to ensure that these personnel operate under the strict management of the Program Manager and do not share their program knowledge with others, except as authorized by the Program Manager. Note also, the Senior Official and CIO may agree to assign CIO personnel to the hub to perform technical analysis and system design activities for the program. In such situations however, knowledgeably of the Program activities by these persons should be clearly delineated, in advance by Program official and CIO.

(U) The Program should be involved in the following activities:

- Initiating and completing any certification and accreditation activities required to deploy UAM software updates;
- Defining, developing, and testing the software logic;
- Preparing software deployment packages for the initial deployment and updates;
- Specifying the UAM data routing requirements to the CIO;

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- Storing and retaining the UAM data;
- Reviewing and analyzing UAM data; and
- Monitoring whether the client is deployed and running to all host computers on the network.

(U) **Coordination and Communication with General Counsel**

(U) Programs should have a close working relationship with the agency General Counsel to ensure all actions taken are legal and within policy. The OGC should review the UAM data information-gathering plans before implementation to avoid spending time and resources on an effort that might later be deemed unauthorized.

(U) The OGC should be responsible for the following activities:

- Reviewing UAM data information-gathering plans before development.
- Occasionally reviewing data produced from UAM to detect unexpected, unintended, and illegal data gathering and use.

(U) The OGC should NOT be involved in the following activities:

- Defining, developing and testing the UAM software logic.
- Analyzing UAM data.

(U//~~FOUO~~) **Steps to Implement UAM**

(U) The following are the basic steps recommended to implement UAM.

1. **Review Policies:** All UAM activities must be covered by agency insider threat policy and the Program implementation plan. If the policies do not cover desirable UAM activities, then action should be taken to update the policies in coordination with the General Counsel, and agency privacy and civil liberties officials.

2. **Evaluate the Current Underlying Information Technology Environment:** UAM requirements are driven by the underlying information technology environment, because it is the activities within that environment that should be monitored. NITTF recommends asking the following basic questions to gain a basic understanding of the environment: Who owns the network? Who controls/manages the network and computers? Where are the computers? How many users are in each environment? How many computers?
3. **Evaluate the Future Underlying IT Environment:** The IT environments supporting many of the classified network environments are continually changing. Cloud technologies and the availability of common services will introduce significant changes in the solutions as they are developed and deployed. The future environment should be considered when developing and implementing a UAM capability.
4. **Establish the UAM Capability:** Using the knowledge of the current and future IT environments, select the software to perform UAM. Then, based on the software, select and implement the information resources necessary to deploy the capability. If the agency is unable to deploy UAM software because of resource limitations or because it is a subscriber rather than an owner of the computers, it will need to implement a service level agreement (SLA) with its service provider to obtain UAM capability.
5. **Identify, Evaluate and Prioritize Potential Insider Threat Conduct:** Behavioral analysis may be important in detecting and deterring anomalous insider threat conduct. NITTF recommends the Program identify insider threat conduct applicable to the agency prior to attempting to deploy host-based software. The result of this step will be an ordered list of behaviors used in developing the UAM data gathering plan, including software logic development.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

6. **Develop a UAM Data Gathering Plan:** The UAM information-gathering plan defines the data of interest and the conditions for collecting the data. A very important aspect of the data gathering plan is the logic used to identify specific conduct of insider threat interest. The UAM plan should be part of the overall Program implementation plan.
7. **Test and Deploy the Capability:** The capability should be tested in an environment that is segregated from any operational or production environment to verify the data gathering requirements are met, including the logic requirements. Next, the capability should be deployed to the operational environment in a controlled, measured approach to mitigate the risk of system failures and negative impact to users.
8. **Send Data to the Program Analytical Hub:** UAM data should be ingested into the Insider Threat Program Office's central analysis hub, where it should be integrated with other data sources for analysis.
9. **Establish Oversight:** Establish an agency oversight mechanism to ensure that all UAM is conducted within applicable laws, regulations, and privacy and civil liberties protections.

(U) The steps to implementing UAM are further expanded in the following pages.

(U) Step 1: Review Policies

(U) The Program should review the agency insider threat policies to make a clear determination that the activities to be performed by the UAM capability are legal, proper and do not violate employee civil liberties. It is likely that policy will need to be continually reviewed and updated to meet the evolving requirements and threats posed by insiders. Subsequently, if policies do not cover the specific activities to be monitored, then action should be taken to update the policies in coordination with the General Counsel.

(U) The following U.S. law and national policies set the framework for UAM:

- Privacy Considerations:
 - *Constitution of United States*
 - *Privacy Act of 1974* (Pub. L. 93-579; 5 U.S.C. 552a)
- Executive Order 12333, *United States Intelligence Activities*, as amended, December 4, 1981
- Executive Order 12968, *Access to Classified Information*, August 4, 1995, revised by Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008 (section 3.5)
- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011
- White House Memorandum on *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 21, 2012
- White House Memorandum on *Compliance with President's Insider Threat Policy*, July 19, 2013.
- Committee on National Security Systems Directive No. 504 *Protecting National Security Systems from Insider Threat*, January 2012

(U) Step 2: Evaluate the Current Underlying Information Technology Environment

(U) The IT professionals working within the Program should evaluate the current underlying IT environment. They may need to seek information from the Office of CIO and security. The evaluation should be conducted with the goal to learn the following:

- Number and location of computers, printers network equipment connected to the classified networks.
- Organizational units that own and operate the equipment.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- Number of network users and a summary of their usage patterns.
- Any SLA or Memorandum of Understanding (MOU) that defines the IT services provided to access the classified networks.
- POCs for supporting organizations.
- Use or availability of software to support UAM.

(U) The characteristics of the current IT environment will affect the design decisions of the UAM capability. The UAM capability will reside in the IT environment, so it is very important to understand how that environment operates and the capabilities being offered. The Program should understand the capabilities of the network, systems, and software available for use and the process for certifying, accrediting and deploying software and systems.

(U) Step 3: Evaluate the Future Underlying Information Technology Environment

(U) The future information technology (IT) environment should be considered when planning a UAM capability. The goal is to understand the architecture and software to be used in the next two to five years and then begin designing a capability that will align with the future and not require significant changes to the capability implemented in the near term.

(U) The IT environments supporting many of the classified network environments are continually changing. For example, many agencies are moving to the Cloud, including software as a service (SaaS), infrastructure as a service (IaaS), elastic storage, and virtual desktops. It is very important that agencies understand the features and capabilities of these new environments to ensure compatibility with the current systems. An agency should seek to develop an immediate UAM solution that has the maximum potential for continued use in any planned future environment.

(U) The IT professionals working within the Program should conduct the evaluation of the future IT

environment. They may need to seek information from the CIO. The evaluation should be conducted with the goal to learn the following:

- What changed in the Service Provider agreements?
 - Will my provider continue?
 - What other options exist?
- Will the number and type of users requiring access to the classified systems and networks change?
- What new technologies or services will impact these users of technologies?
 - Wireless networks
 - Mobile devices
- How will available UAM software solutions continue to evolve?
- How will the architecture and solutions offered by your service provider change?

(U) Step 4: Establish the UAM Capability

(U) Using the knowledge of the current and future IT environments, the Program should establish the IT resources required to support the UAM capability. A primary task in this step should be to select the software to perform UAM. Then, select and implement the information resources necessary to deploy and operate the software.

(U) The Program should be prepared to make the following decisions:

- What UAM software will to be used, or integrated into via hybrid service relationship
- What network location will UAM data be stored
- What amount of storage will be procured
- What hardware and software will required to operate the capability

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) The IT professionals working within the Program should consider the findings from evaluations of both the current and future IT environments when making the UAM capability decision. The following issues should be given consideration when selecting UAM software:

- Requirements coverage
- Require additional software development required?
- Total cost of ownership (initial + operating costs)
- Alignment of the software solution's product roadmap to the future technology environment and Program goals
- Performance history of the solution (who else is using it, where limitations exists, what problems are occurring)
- Difficulty to change the solution later
- Continuity of Operations Planning
- Disaster recovery strategy

(U) If agencies are unable to deploy UAM software because the agency is a subscriber and is not owner of the computer system, it will need to implement a service level agreement (SLA) with its service provider to obtain UAM capability. More information about establishing an SLA is provided in the Service Level Agreements section below.

(U) Service Level Agreements



(U) Service Providers

(U//~~FOUO~~) The assumption should NOT be made that because another agency owns or operates a system or network that agency is performing user activity monitoring for its various client agencies. Experience has shown that this is not the case, even where a service provider is conducting UAM of its employees on the same system.

(U) Agencies that are subscribers to networks owned or operated by another agency (called a service provider) will need to establish an SLA or MOU with their provider to detail how UAM data will be collected and transmitted to the subscriber.

(U) The SLA should focus on establishing accountability for the UAM service to be provided to the subscriber. The service provider should be responsible to provide data about the following user activities:

- All types of data removal
- All types of data reproduction
- All types of data access
- All types of data transmission
- All types of search

(U) SLAs should be negotiated with the service provider before a UAM solution is implemented. SLAs should:

- Identify the UAM software that the service provider employs;
- Define costs and terms;
- Document the responsibilities of all parties;
- Define the start of the agreement, its initial term, and the provision for reviews;
- Define in detail the service to be delivered by the service provider and the level of service the subscriber can expect;
- Institute a clear, formal, and accountable list of tasks to be performed by service provider;
- Provide a common understanding of service requirements/tasks and the organizations/teams involved in performing those services;
- Provide for all parties a single reference describing all objectives and listing the following types of information:
 - Description of the service
 - Agreed service hours

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- Reliability or warranty
- Customer support (who to contact, how, priority, response times, etc.)
- Change management procedures (who has authority to make a change)
- Service continuity (e.g., COOP)
- Frequency of UAM (e.g., near-real-time)
- Frequency of reporting (e.g., daily)
- Data format (e.g., XML, LOG .txt (ASCII typed files or ZIP binary)
- Delivery mechanisms (i.e. network or DVD ROM physical media)
- Provider Incident Response POC
- Subscriber Incident Response POC
- Uptime/quality of service objective (e.g., 99.999%)
- Data accessibility requirements, if applicable
- Length of data accessibility, if appropriate
- Data Protection and safeguarding requirements
- Accessing or attempting to access websites, files, and data beyond the scope of the individual's responsibilities and need-to-know
- Adding user accounts used later to access systems
- Reviewing or manipulating system log files
- Downloading large number of files
- Remotely accessing the system and performing tasks atypical to their responsibilities, typically after business hours
- Writing scripts to delete, modify, or move files
- Copying data to removable media without authorization
- Sending classified documents to persons without a need to know or the proper security accesses/clearance
- Accessing systems remotely
- Elevating or assigning administrator roles to unauthorized users or accounts
- Changing the permissions of files and folders
- Accessing another user's computer when left unattended
- Printing documents to a printer at a location that differs from location of the host computer
- Failing to follow policies and controls
- Copying a larger number of files to a laptop computer over a short or long period of time
- Accessing users' and administrators' accounts after termination of employment
- Having been recently terminated, disciplined, demoted or changed duties/roles
- Communication, in any form, regarding disgruntlement over an action or policy
- Using computer resources to conduct a side business

(U) Step 5: Identify, Evaluate, and Prioritize Concerning Insider Threat Conduct

(U//~~FOUO~~) The Program personnel should identify user conduct consistent with the known patterns of malicious activity. The UAM plan should be designed to capture the data needed to identify this conduct. Agencies are encouraged to identify insider threat conduct patterns that apply to their users by reviewing known insider threat cases. The following list of insider threat patterns of activity was culled from known insider threat cases provided in the CERT's *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (see [Helpful References, page 3](#)). The list is not inclusive all of all insider threat conduct:

- Accessing, without proper authorization, proprietary or classified information in the 30 days prior to termination of employment

UNCLASSIFIED//~~FOUO~~

- Associating with known criminals or suspicious persons
- Attempting to gain employees' passwords or obtain access through trickery or exploitation of a trusted relationship

(U//~~FOUO~~) **An Example of Potential Malicious Conduct:** An example of potential malicious conduct is represented in the graphic above. "User A" logs onto a workstation at a location different from the location of the most recent badge in. This may indicate that a user is using another person's account or badge. This could be an effort to conceal malicious activity. Furthermore, the same user e-mails a large number of files to an external e-mail address. This may indicate that a user is trying to exfiltrate proprietary or classified information.

(U) An effective practice of established Insider Threat Programs is to gather the Program personnel on a regular basis to brainstorm threats that

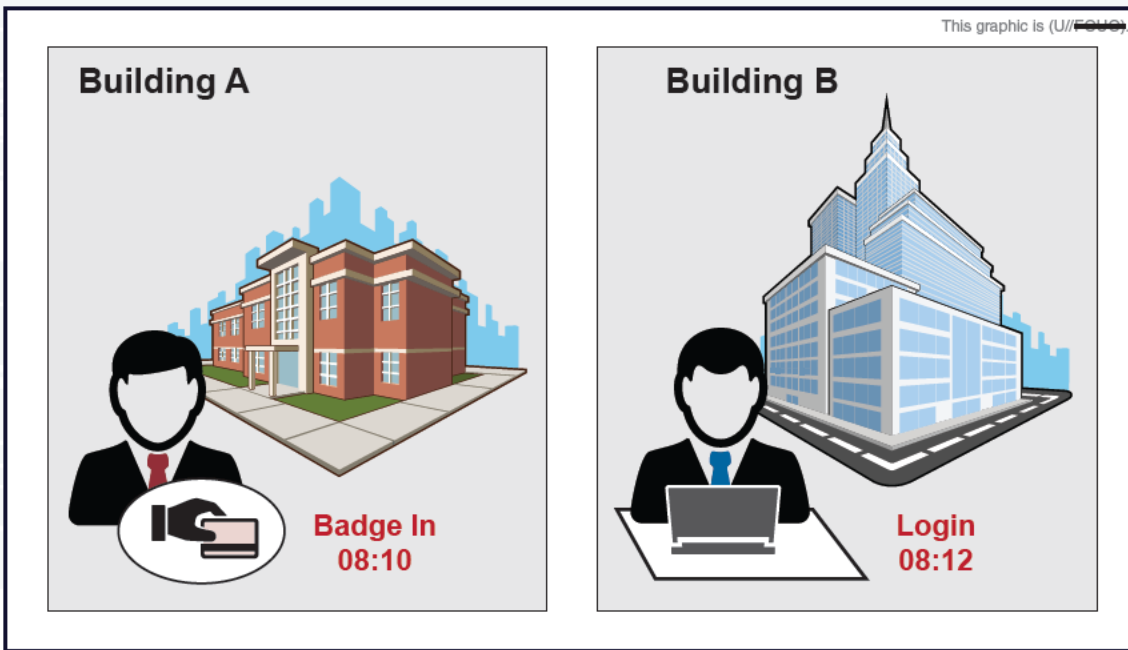
insiders may pose to their organization. Here are some questions that should be considered:

- "If I wanted to exfiltrate classified information without getting detected, how would I go about that?"
- "If I wanted to damage the operational capability of my agency's networks and computers without getting caught, how would I do that?"
- "How could a foreign intelligence service use an unwitting insider to gather information or cause damage to networks and computers?"

(U) Step 6: Develop an Information-Gathering Plan

(U//~~FOUO~~) The UAM plan, as part of the overall Program implementation plan, should define the data to be gathered to detect insider threat conduct. UAM is most

(U//~~FOUO~~) **Figure 3: Malicious Behavior**



(U//~~FOUO~~) Potential behavior of concern: an individual logs in to a computer located in a facility other than where the person has badged in.

UNCLASSIFIED//~~FOUO~~

effective if it is designed to capture data about user activities that reflect the concerning conduct (habits, techniques, and tradecraft) of insiders identified in the previous step. The Program should include a team of analysts, behavioral specialists, and IT professionals to develop the UAM plan. The plan should define the data to be collected to support the analytic approach employed in the analytic hub to detect insider threat conduct. IT professionals add value to this process because they have a strong understanding of the user activities that are available to capture on a host computer for each targeted user behavior. The behavioral specialist will aid in the translation of the insider threat conduct identified in Step 5 (see page 43). The analysts will help identify how the data will be used. The roles of these professionals should be consistent with the Program's plan to control and limit the exposure of the UAM plan.

(U//~~FOUO~~) **The recommended processes to identify, implement, and refine the UAM plan are:**

- Determine classes of users to be monitored
- Identify User Activities
- Implement Information-Gathering Methods
- Refine Plan

(U//~~FOUO~~) Originate groups of users to be monitored: Each agency should assess whether users with elevated access or privileges -- privileged users, (PU) -- will be monitored differently than the typical (non-privileged) user. PU may have the ability to overcome protection measures, change software configurations, and change the access of users or programs. Therefore, PU pose a higher risk and may warrant closer UAM. Also, each agency may want to implement an increased level of UAM for users who are officially under investigation. The determination of how users will be categorized and the users to be included in these categories should be governed by policy and adequately protected.

(U) **The following steps to develop the plan must be performed for each user group created.**



(U//~~FOUO~~) Sensitive Nature of the UAM Plan

(U//~~FOUO~~) The UAM Plan should be classified per the *Insider Threat Security Classification Guide*, presently under development by FBI and ONCIX, as Co-Directors of the NITTF. Details of the plan, particularly the logic, may reveal tactics, techniques, and procedures and may need to be classified. It is possible that UAM will be conducted on unclassified networks. In that case, the implementation of a UAM plan on an unclassified network should be protected in a manner to prevent disclosure of classified information.

(U//~~FOUO~~) 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 must therefore be monitored with diligence.

(U//~~FOUO~~) **Identify User Activities:** The approach to identifying the user activities should begin with the list of concerning insider threat conduct identified in Step 5. For each concerning behavior the team should determine what computer user activity will indicate the subject conduct is occurring. For example, if a concerning insider threat conduct is "excessive printing of classified documents" the following computer user activities may be of interest:

- All print activity
- Print activity specific to documents or material that is classified
- Copy and paste activities to remove or obfuscate the classification of a document

(U//~~FOUO~~) UAM data gathering is best organized into two categories: basic and advanced. The differences of the two categories are explained:

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- **Basic UAM** information-gathering collects and stores ALL of the activities in a general category without logic. For example, collect data every time a user prints a document and collect data every time a user logs into the host computer. Basic information-gathering may be needed to support network and pattern analysis with the larger, integrated dataset in the analytic hub.
- **Advanced UAM** information-gathering applies logic to one of more details about a user activity. For example, collect data about a print job and the document being printed WHEN the document contains specific keywords, perhaps a classification level. Advanced information-gathering produces more meaningful alerts of potential malicious conduct.

(U//~~FOUO~~) The team should attempt to implement advanced information-gathering in order to produce data that is more valuable and meaningful to the analysts. The ability to implement advanced information-gathering directly depends upon the capabilities of the UAM software and the type of activities to be monitored.

(U//~~FOUO~~) **Implement Information-Gathering Methods:** The specific approach to implement basic and advanced data gathering is highly dependent upon the UAM software. However, the following details should be included in each information-gathering implementation:

- Identifier of the subject or actor (e.g., the name or userID of the individual user)
- Date and time of the event using common date and time of network
- Type of event
- Details of any object
- IP and MAC address of the host to determine location

(U) The UAM plan should be implemented in a test environment that is separate from the operational or production environment. The test environment should

be within the UAM private enclave. This is a standard precaution in system development practices to control the environment where the tests are being conducted while protecting the operational environment from being impacted by untested software and systems. This environment will be referred to as the "Pilot/Lab."

(U) Functional tests should be conducted on the implementation to evaluate if the software collects the activity as defined in the plan.

(U//~~FOUO~~) **Refine Plan:** An important characteristic of an effective UAM Plan is continual improvement. The conduct of malicious insiders will constantly evolve and adapt. Therefore, the insider threat detection program, specifically the UAM plan and analytical approach, should continue to adapt. The Program should regularly evaluate the effectiveness of the plan. The following questions should be considered:

- Is the data produced helpful?
- Is additional data required to support advanced analytical requirements?
- Have additional activities of concern been identified?

(U) The answers to these questions may necessitate updates to the UAM plan.

(U) **Step 7: Test and Deploy the Capability**

(U) The Program will be responsible for preparing the software for deployment, including the delivery of software configuration files to the CIO deployment team. The CIO staff will be responsible for deploying the software and configuration files in a systematic phased method to meet the requirements of the phased deployment plan.

(U//~~FOUO~~) The execution of UAM software on host computers can require a significant amount of processor, memory, network and storage resources. The increased demand for these resources can produce a negative impact on users and systems across any enterprise. Therefore, the deployment of UAM software

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

should be conducted in a careful, incremental approach that includes functional and performance testing designed to minimize risks. Agencies with established insider threat Programs use an approach that deploys the software and updates to an incrementally larger user population in each phase. The goal of this approach is to accomplish full deployment while minimizing the risk that that user experience is negatively affected or network performance is adversely degraded.

(U//~~FOUO~~) This approach was developed and then revised by several agencies as they implemented their insider threat programs. The approach has 4 phases:

- Phase 0: Pilot/Lab Deployment
- Phase 1: Initial Operating Phase
- Phase 2: Local Full-Enterprise
- Phase 3: Enterprise-wide

(U) UAM software should be tested against performance standards during each phase of the deployment. The performance standards should be defined in advance with some coordination with the CIO. This approach incrementally increases the scope of the deployment in each phase to minimize the risk of negative impacts. Performance testing will evaluate the impact of the UAM software on the IT resources. The testing should evaluate how the processor, memory, and network resources on the user's computer are impacted by the UAM software under a variety of circumstances. Performance evaluation should also assess the impact on network and database/storage. Performance control gates should be assigned to each phase to enforce the standards.

(U) **Phase 0: Pilot/Lab Deployment:** The goal of Phase 0 is to evaluate the functionality of the UAM software and the performance of the computers and network in a non-operational or test environment. The functionality tests will assess whether the UAM software collects the data per the defined plan requirements. For example, if the information-gathering plan includes a requirement to collect each time a user prints a document, then the tests will effectively evaluate

several scenarios to that effect. The performance of the computers will be compared to known baseline of activities. For example, the amount of time to conduct the following actions on the computer should be evaluated: logon, print a document, send an e-mail, open e-mail, open Microsoft Word, and save a file from an e-mail. Use of a test environment will restrict the potential impact of the software on other systems.

(U) **Phase 1: Initial Operating Phase:** The goal of Phase 1 is to evaluate the functionality and impact of the UAM software on a small number of users on the operational or production system. Deploy to 10% of the entire planned user population. The desired outcome is approval to proceed to the next phase.

(U) **Phase 2: Local Partial-Enterprise:** The goal of Phase 2 is to evaluate the functionality and impact of the UAM software when deployed to a sizeable number of users. Deploy to 40 percent of the entire planned user population. The outcome is approval to proceed (may require some certification and accreditation approval)

(U) **Phase 3: Enterprise-wide:** The goal of Phase 3 is to evaluate the functionality and impact of the UAM software to the entire enterprise. Deploy to 100 percent of the entire planned user population. The desired outcome is the completion of enterprise-wide deployment.

(U//~~FOUO~~) Step 8: Send Data to the Program Hub

(U//~~FOUO~~) The primary outcome of the UAM software is data that will be ingested into the hub for processing and analysis. Processes should be established and outlined in the agency's Insider Threat Implementation Plan to ensure this flow occurs. As stated in the Policy and Standards (paragraph E.1), UAM data will be one of many data sources moved into the Insider Threat hub. Additionally, the UAM data should flow into a permanent read-only repository as the system of record to support future investigations or analysis. Agencies should address both these issues within their insider threat hub IT infrastructure and within the Program Implementation

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Plan. Agency Record Management expertise will be required to ensure that UAM data is retained consistent with agency and records guidelines (see *Record Management Requirements*, page 10).

(U//~~FOUO~~) The amount of UAM data is likely to be very large. In the hub, it will gain value as it is combined with other data and analyzed. UAM data alone will not detect insider threats; rather, it detects patterns of activity that indicate conduct matching to known insider threats.

(U) Step 9: Oversight

(U) The direct responsibility for UAM falls on the designated Senior Official and should not be delegated. The Senior Official should oversee all activities of the Program, including UAM. Additionally, the agency head is required by the Policy and Standards to include a mechanism that involves the employment of program UAM as well as oversight that employs periodic reviews by cleared evaluators selected by the agency head and drawn from sources external to the program itself.

(U//~~FOUO~~) The Program office should ensure the following UAM policies are included in the agency's insider threat policy approved by the agency head.

- **User Notification:** A policy defining how the users are notified of their right to privacy, and that their activities on the IT systems are monitored through banners, signed user agreements and rules of conduct.
- **User Activity Data Gathering:** A policy defining the data that may be collected, data classification, and retention requirements in accordance with applicable standards (e.g., *Committee on National Security System Directives and Instructions*; *National Institutes of Standards and Technology Security Controls*; *National Archives and Records Administration directives*; and Policy and Standards). The UAM Information-Gathering Plan will implement this policy.

- **Chain of Custody:** A policy controlling access to data to preserve data integrity for admissibility in court.
- **System of Record:** A policy defining whether the UAM component repository is the system of record. The determination should be made in close consultation with agency record management officials.

(U) Definitions Related To UAM

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

(U) **Conduct:** Observable activities of a person (user).

(U) **Data access activities:** Attempts or action, successful and unsuccessful, to open or execute a computer file, or view the properties of the computer file.

(U) **Data removal activities:** Attempts or action, successful and unsuccessful, to copy a file to removable media (CD, USB, DVD).

(U) **Data reproduction activities:** Attempts or action, successful and unsuccessful, to copy a file to another storage location (local drive, shared drive, network drive, website).

(U) **Data transmission activities:** Attempts or action, successful and unsuccessful, to send a file to another user via e-mail, FTP, or HTTP.

(U) **Enclave:** A set of information and processing capabilities that are protected as a group. The capabilities may include networks, hosts, or applications. Enclaves are required when the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment.

(U) **Enterprise Audit (EA):** An independent examination of records and activities, employed by the Chief Information Officer of an agency, to assess the

UNCLASSIFIED//~~FOUO~~

adequacy of system controls on computer systems operated by that agency and to ensure compliance with established policies and operational procedures.

(U) **Host:** A host is a computer connected to a network and may offer information resources, services, and applications to other computers on the network.

(U) **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.

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

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

(U//~~FOUO~~) **Service Provider:** The agency providing the classified network service to another agency. The owner and operator of a classified system issued to and used by another agency.

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

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

(U) **User Activity Monitoring (UAM):** 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.

- Activities include, but are not limited to:
 - keystrokes, copy and paste, printing, viewing document content, web browser use, e-mailing, messaging, and use of removable media.
- Observe and record the format of text descriptions, screen capture, and full-screen video capture.
- UAM is near real-time.
- UAM operates in conjunction with inputs from other data sources such as enterprise audit and continuous monitoring.

UNCLASSIFIED//~~FOUO~~



UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) Appendix A: Guidelines for Media Interface

(U) As an agency begins to implement its Program, it probably will develop a relationship with the NITTF, particularly if the NITTF directly assists an agency in establishing its program. As the agency program develops, and becomes a matter of public record, that fact may generate new interest on the part of the public and news media. The following guidelines provide useful information about the NITTF and insider threat programs, in general, that may provide an agency with the content through which to appropriately address public and media inquiries.

(U) Mission Statement

(U) The NITTF assists federal agencies with developing insider threat programs to prevent, detect, and deter compromises of classified information by insiders. The NITTF goal is to protect classified information from people, groups and nations that can harm the national security of our country.

(U) Background

(U) The release of hundreds of thousands of classified and sensitive U.S. Government documents through the WikiLeaks internet site demonstrated to the government and the public that current sharing and safeguarding procedures for classified information were inadequate and put our nation's security at risk. In response, President Obama in October 2011 issued Executive Order (E.O.) 13587 *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* to improve the security of classified computer networks and classified information. As part of the E.O. 13857, the President directed all Federal Departments and Agencies to institute insider threat detection and

prevention programs, and established the NITTF under the joint leadership of the U.S. Attorney General and the Director of National Intelligence (DNI) to assist agencies in developing and implementing their insider threat programs. In developing standards for these programs, the task force specifically sought to ensure they not erode civil liberties, civil rights, or privacy protections for government employees. In November 2012, following an extensive interagency coordination and vetting process, the President issued the *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs* memorandum. The E.O. 13587 charged the NITTF with designing and implementing insider threat policies and standards that take into account the mission risks and resources of affected agencies and departments. While developing ways to protect classified information, the NITTF is also ensuring that insider threat program measures maintain the civil liberties and privacy protections due government employees.

(U) Talking Points and Possible Questions

(U) *Who runs the NITTF, and which agencies are involved?*

(U) Under the E.O. 13587, the U.S. Attorney General and the DNI are NITTF co-chairs. They designated the Federal Bureau of Investigation (FBI) and the National Counterintelligence Executive to co-direct the daily activities of the NITTF. Employees and contractors from a variety of federal agencies comprise the NITTF, and its services impact more than 70 federal agencies that handle classified material. It reports directly to the Information Sharing and Safeguarding Steering Committee, which the President established under E.O. 13587. The steering committee is largely made up of Intelligence Community agencies. It includes representatives from the Departments of State, Energy, Justice, Defense, and Homeland Security; CIA; FBI; the

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Office of the Director of National Intelligence (ODNI); the ONCIX; the Information Sharing Executive; the National Security Agency; Office of Management and Budget; the National Security Staff; the Defense Intelligence Agency; and the Information Security Oversight Office.

(U) *Is this new push going to impinge on anyone's civil rights?*

(U) The Government's efforts are guided by the *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs* and do not mandate reporting by employees on their fellow employees. They do, however, mandate training and awareness. The training simply educates employees about when activities or behavior observed might be indicative of insider threats or, at the very least, suggestive of improper activity (criminal or not). The awareness piece is intended to raise the awareness of these cleared employees whose classified placement and access make them the possible targets of foreign intelligence and security services. These do not require special talents. Just as if in the course of normal duties, an employee was to see someone removing classified documents that they should not be removing, for example, especially if this happens multiple times, without apparent reason, and the person appears nervous, that is suspicious activity that should be reported. The agency insider threat Program team then looks at the facts surrounding that activity and determines recommendations for actions that may be appropriate and necessary to respond to the reported activity. It is not that different from the situation where an employee sees someone with a suspicious package at a subway station, and reports it. Same thing. In past espionage cases, witnesses saw things that may have helped identify a spy or other malicious insider, but never reported them. In many cases they were unaware of the possible significance or relevance of what they had observed. That is why the awareness effort of the program teaches not only what types of activity to report, but how to report it and WHY it is so important to report it.

(U) *Why was the NITTF set up?*

(U) The NITTF was set up in response to the WikiLeaks public release of thousands of classified documents. The NITTF develops national insider threat policy and

supporting standards and guidance designed to help prevent a similar incident, or any other unauthorized disclosures of classified information.

(U) *What is an insider threat?*

(U) The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. An insider is an entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. Whistleblowers are not insider threats and are protected under federal statutes.

(U) *How does the NITTF operate?*

(U) The NITTF draws expertise from across the government in areas of security, counterintelligence, and information assurance in order to develop the policies and standards necessary for agencies to implement insider threat detection and prevention programs. A significant part of the NITTF effort involves assisting with educating and training personnel to recognize insider threats, without creating an atmosphere of distrust. After the NITTF implements the programs in each agency, the NITTF may evaluate the insider threat programs within individual Departments and Agencies. While interfacing with individual agencies, the NITTF will identify and share best practices for detecting and deterring emerging threats, and continue to assist agencies in resolving issues.

(U) *How do you detect an insider threat?*

(U) Detecting potentially damaging behavior among employees with access to classified information involves gathering and analyzing information from many sources for behaviors of concern. Depression, alcohol or drug use, personal stress, financial trouble, and being disgruntled with an employer are all indicators that have appeared in actual espionage cases. Combining these indicators with other behaviors like working unexplained hours, accessing information unrelated to an employee's job, a sudden increase in wealth, or

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

displaying unusual behavior on the agency network, for example, could suggest a threat. An insider threat Program combines relevant information from multiple sources to determine if an employee deserves closer scrutiny or if the matter should be formally brought to the attention of an investigative or administrative entity, such as the FBI or an inspector general. Fortunately, it is rare to find reasons to suspect a federal employee of being an insider.

(U) *Is every agency required to implement the new procedures and security applications?*

(U) Every executive agency with employees who access classified information is required by the E.O. 13857 to implement and maintain an insider threat program.

(U) *Is there any way to stop an insider threat?*

(U) There is no fool-proof method that will work in all cases. One way to increase the odds of catching a insider is to examine relevant information regarding the behavior of those who access classified information and then act to resolve concerns as soon as possible. This is what insider threat programs attempt to do. For example, an agency may identify inappropriate employee activity on computers and through other traceable means that produce red flags. When those flags appear the agency can begin looking more closely into the employee's behavior. The agency can combine flags and anomalies with information from other files, records, and sources to see if patterns suggest behaviors of serious concern. An insider threat program also seeks to better educate workforces about behavior that might be consistent with an insider threat and how to report such behavior.

(U) *Is this new push going to impinge on anyone's civil rights?*

(U) Government employees who are authorized to handle classified information understand and accept the additional oversight of their workplace activities. Employees often sign waivers before beginning employment, and warning banners on computers and in facilities remind employees that their activities are subject to monitoring. Employees should know that if they are doing nothing wrong they have little to worry about. The goal is to deter or detect only the people who pose a threat to national security.

(U) *What harm can someone do to our government based on the unauthorized release of classified information?*

(U) The reason information is classified is to restrict the information to only those who require it to support our national security objectives. When people divulge classified information outside the confines of the U.S. Government national security structure, the contents of that information can create situations that are harmful to U.S. interests and, in some cases, be potentially life-threatening. Classified information in the wrong hands can provide a unique and potentially dangerous advantage to states and non-state actors whose interests are opposed to ours. For example, classified information can provide details about the vulnerabilities of our most sensitive weapons systems, which could be used to defeat those weapons or render them less effective; provide information about our adversaries' intentions and U.S. plans to counter their actions; provide sensitive information about the identity, location, and future plans of terrorist organizations; be used to produce nuclear, chemical, and biological weapons; identify critical weaknesses in the national infrastructure that, if exploited, could damage internal U.S. transportation, health, and communications capabilities.

(U) *What happens to an employee who is accused of releasing unauthorized classified information?*

(U) Possible responses range from being reprimanded to being prosecuted for violation of a criminal statute. Each case has different factors that determine the course of action an agency takes.

(U) *How long will the NITTF exist?*

(U) The NITTF will be in place until the applicable agencies formally adopt the *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs* and until the President determines that the assistance and assessment work of the NITTF has concluded.

(U) *Need additional information?*

(U) Additional assistance may be obtained from NITTF at (b)(3) the FBI Public Affairs Office (b)(6) or the ODNI Public Affairs Office (b)(3)

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

(U) Appendix B: Agency Policy Template

(U) INSIDER THREAT PROGRAM DRAFT POLICY TEMPLATE

(U) *The following template is offered as a starting point for agencies to craft internal insider threat policies that are relevant to the unique environment of each individual agency. Additional assistance and reference documents can be obtained from the National Insider Threat Task Force (NITTF) at (b)(3) (classified) or (b)(3) (unclassified).*

(U) AUTHORITY: Executive Order (E.O.) 13587 *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; E.O. 12333 *United States Intelligence Activities*; E.O. 10450 *Security Requirements for Government Employees*; E.O. 13467 *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security*; E.O. 13526 *Classified National Security Information*; E.O. 12968 *National Industrial Security Program*; White House Memorandum on *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs*, dated 21 November 2012.

(U) PURPOSE. Under the authorities vested in [Department/Agency (D/A), as appropriate Director], by [Site D/A Governing Documents], E.O. 13587 directs structural reforms to improve security of classified networks and responsible sharing and safeguarding of classified information. The E.O. 13587 applies to all departments and agencies that access and/or maintain classified material and/or classified information systems and all individuals assigned thereto with access to same. The policy:

- Establishes and assigns responsibilities for D/A Insider Threat Program (“Program”).
- Establishes authorities and relationships specific to the implementation and oversight of the program.
- Directs the integration of counterintelligence (CI), information assurance (IA), antiterrorism, force protection, security/law enforcement, and human resources (HR); information for the purpose of insider threat detection and prevention.
- Directs material support from and coordination with D/A legal and civil liberties entities.

(U) APPLICABILITY: This policy applies to all personnel. The policy requires specific action by all D/A programs, locations, and employees (including personnel employed under contract by the D/A).

(U) REFERENCES:

- A. *U.S. Government Insider Threat Detection Guide, 2011**
- B. White House Memorandum on *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs*, dated 21 November 2012
- C. *Counterintelligence/Security Risk Assessment Framework for Federal Partners*, dated March 2012
- D. *Defensive Counterintelligence Program Blueprint—2010*
- E. DEPARTMENT/AGENCY (D/A) _____
INSIDER THREAT POLICY

^dThis is classified document.

UNCLASSIFIED//~~FOUO~~

~~(U//FOUO)~~ **POLICY:**

(U) The D/A head shall establish a program for the D/A and all subordinate elements to prevent unauthorized disclosure of classified information, deter cleared employees from becoming insider threats, detect employees who pose a risk to classified information, and mitigate the risks to the security of classified information through administrative, investigative or other responses.

(U) All D/A offices shall establish procedures within their respective offices to ensure that information is accessible to and shared with insider threat program personnel for the purposes set forth in this policy.

~~(U)~~ **SENIOR OFFICIALS RESPONSIBILITIES:**

(U) (***)Considerations: The Senior Official responsible for the insider threat Program should be experienced in the Security and Counterintelligence disciplines and work closely with the Chief Information Officer (CIO), as well as the HR, Antiterrorism/Force protection, Law Enforcement, and Legal/Civil Liberties entities (as applicable and relevant), in the coordination of activities in support of this policy. (***)

(U) The (ENTER TITLE of D/A head) is responsible for establishing, within the D/A, an insider threat detection and prevention program.

~~(U//FOUO)~~ The (ENTER TITLE) is hereby designated the Senior Official responsible for providing the management, accountability and oversight of D/A insider threat program, as well as provide resource recommendations to D/A head. The Senior Official shall:

~~(U//FOUO)~~ Develop and promulgate a comprehensive agency insider threat policy and implementation plan, to be approved by the agency head within 180 days of the effective date of the national insider threat policy.

~~(U//FOUO)~~ Annually report to the D/A head program progress and/or status within D/A. Annual reports shall document annual accomplishments, resources allocated, insider threats identified, program goals, impediments and/or challenges.

~~(U//FOUO)~~ Collaborate with D/A General Counsel and appropriate privacy and civil liberties officials to ensure that all insider threat program activities are conducted in accordance with applicable laws and privacy & civil liberties policies.

~~(U//FOUO)~~ Establish oversight mechanisms or procedures to ensure proper handling and use of records and data described below and ensure access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.

~~(U//FOUO)~~ Ensure the establishment of guidelines and procedures for the retention of records and documents necessary to document D/A activities required by E.O. 13587.

~~(U//FOUO)~~ Facilitate oversight reviews by cleared officials designated by the D/A head to ensure compliance with national and D/A insider threat policies and standards.

~~(U)~~ **INFORMATION INTEGRATION, ANALYSIS AND RESPONSE:** The Senior Official shall:

(U) (***)Considerations: Integrate resources; Ensure data gathering complies with rules and reporting processes established for each program detection capability component; Establish an analysis, reporting, and response capability to support insider threat detection. In doing, correlate in a central location and analyze, when available, the following information to identify anomalous behavior that may reveal insider threat activity: Information collected from audit data; Foreign travel & foreign contact data; Polygraph screening and vetting data; Financial disclosure data; and Personnel security vetting data. Also, ensure best practices of DA's CI, Security, IA & HR organizations are shared. As appropriate, the offices of the Inspector General/legal counsel, civil liberties and staff of the employee assistance program should be included in reviews of best practices. (***)

~~(U//FOUO)~~ Establish an insider threat program office with an analytic response capability to manually and/or electronically gather, integrate, review, assess and

UNCLASSIFIED//~~FOUO~~

respond to information derived from CI, Security, IA, HR, Law Enforcement, the monitoring of user computer activity, and other information sources as deemed appropriate.

(U//~~FOUO~~) Ensure the insider threat program office establishes procedures for D/A insider threat response action(s), such inquiries, to clarify or resolve insider threat matters. Procedures will ensure that response action(s) are centrally managed and documented by the insider threat program office.

(U//~~FOUO~~) Ensure insider threat program office establishes access to the behavioral science services of a psychologist either on staff, under contract, or via agreement with another federal agency. This individual should have experience in counterintelligence, security, or insider threat and be able to provide consultation, research and/or training.

I. (U) TRAINING OF INSIDER THREAT PERSONNEL:

The Senior Official shall:

(U) (***)Considerations: Agencies should consider providing tailored training to certain higher risk personnel depending on mission, access and vulnerabilities as follows: CI and Security Personnel; Supervisors and managers; Insider threat detection program leads; Information assurance, IT systems administrators and engineers, and IT close support team members; Employees cleared for Special Access Programs and other compartmented programs; and Investigators and personnel security adjudicators. (***)

- A. (U//~~FOUO~~) Ensure insider threat program personnel are appropriately trained in counterintelligence and security fundamentals as well as in D/A procedures for conducting insider threat response actions.
- B. (U//~~FOUO~~) Ensure insider threat program office provides training in applicable laws and regulations governing privacy and civil liberties; safeguarding of records and data, including the consequences of misuse of such information; and the 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 FBI, the Department of Justice, or military investigative services.

II. (U) ACCESS TO INFORMATION: The Senior Official shall:

(U) (***)Considerations: Agencies may want to consider establishing an Insider Threat Working Group, led by a designated Senior Executive, to ensure appropriate policies, objectives and priorities as it relates to access to and sharing of pertinent information CI, security, IT and HR data in furtherance of program development, implementation, management and oversight. (***)

- A. (U//~~FOUO~~) Direct all D/A elements, including, but not limited to CI, Security, IA, HR 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. Reporting guidelines shall also be established for these components D/A elements to ensure that relevant information is directly and regularly accessible by the insider threat program office. Such information includes, but is not limited to:
 1. (U//~~FOUO~~) Counterintelligence/Security. All relevant databases and files to include but not limited to personnel security files, law enforcement files, polygraph examination reports, facility access records, security violation files, foreign travel records, foreign contact reports, and financial disclosure filings.
 2. (U//~~FOUO~~) 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, enterprise audit, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.
 3. (U//~~FOUO~~) Human Resources. All relevant HR databases and files to include but not limited to,

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

personnel files, payroll and voucher files, outside work/activities requests disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

- B. (U//~~FOUO~~) Ensure the insider threat program office establishes procedures for access requests by the insider threat program involving particularly sensitive or protected information, such as information held by law enforcement, Inspector General, or other investigative sources.
- C. (U//~~FOUO~~) Ensure the insider threat program has timely access as otherwise permitted, to available U.S. Government intelligence and counterintelligence reporting information and analytic products relative to foreign intelligence services and other adversarial threats.

III. (U) MONITORING USER ACTIVITY ON NETWORKS: The Senior Official shall:

(U) (***)Considerations for Auditable User Events: logons/logoffs; file and object access; user and group management; security & audit policy changes; system restarts/shutdowns; file and object manipulation such as addition, deletion, modification, to include change of permissions and/or ownership; print activity; use of privileged/special rights; writes/downloads to local devices such as USB drives, DVDs and CD-ROMs; uploads from local devices; file(s) printed to include descriptive information, enabling identification of printed item; root level access; query strings; and query results.***)

- A. (U//~~FOUO~~) Either internally or via agreement with external agencies, develop a capability 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 insider threat personnel.

B. (U//~~FOUO~~) Develop and implement policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

C. (U//~~FOUO~~) Ensure agreements are signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include government portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be developed in close consultation with legal counsel.

D. (U//~~FOUO~~) Ensure use of classified and unclassified network banners shall be employed within the D/A informing consenting users that the network is being monitored for lawful U.S. Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be developed in close consultation with legal counsel.

IV. (U) EMPLOYEE TRAINING AND AWARENESS: The Senior Official Shall:

(U) (***)Recommendations for Employee Training: All employees should receive annual training. Agencies should work together to share briefings and materials, seek out assistance on mentoring and share training models, methodologies and best business practices. Points of training emphasis should be on behavioral issues; espionage indicators; substance abuse and mental health issues; inappropriate interpersonal behavior; hostile or vindictive behavior; criminal behavior; finances; foreign contacts and foreign travel; mishandling of classified and security violations; divided and/or conflicted loyalty to the U.S. Further, the following training awareness methods should be considered: formal classroom training to include refresher briefing, computer-based training, awareness videos, and automated e-learning course.***)

- A. (U//~~FOUO~~) Ensure insider threat awareness training, either in-person or computer-based, is provided

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

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:

1. (U//~~FOUO~~) The importance of detecting potential insider threats by individuals with access to classified information and reporting suspected activity to appropriate insider threat or security offices;
2. (U//~~FOUO~~) Methodologies of foreign intelligence entities to recruit sources and collect classified information;
3. (U//~~FOUO~~) Indicators of insider threat behavior, and procedures to report such behavior; and
4. (U//~~FOUO~~) Counterintelligence and security reporting requirements, as applicable.
5. (U//~~FOUO~~) Privacy and civil liberties instruction, as pertains to the D/A insider threat policy and program.

B. (U//~~FOUO~~) ensure insider threat programs do the following:

1. (U//~~FOUO~~) Verify that all cleared employees have completed the required insider threat awareness training contained in these standards.
2. (U//~~FOUO~~) 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.

(U) **DEFINITIONS:**

(U) "Agency Head" means the head of any: "Executive agency," as defined in 5 U.S.C. §105; "military

department" as defined in 5 U.S.C. §102; independent establishment" as defined in 5 U.S.C. §104; intelligence community element as defined in E.O. 12333; and other entity within the Executive Branch that comes into the possession of classified information.

(U) "Classified Information" means information that has been determined pursuant to E.O. 13526, or any successor order, E.O. 12951, or any successor order, or the *Atomic Energy Act of 1954* (42 U.S.C. 2011), to require protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form.

(U) "Cleared Employee" means a person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

(U) "Insider Threat" means the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

(U) "Insider Threat Response Action(s)" means activities to ascertain whether certain matters or information indicate the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of counterintelligence, security, law enforcement, or Inspector General elements depending on statutory authority and internal policies governing the conduct of such in each agency.

UNCLASSIFIED//~~FOUO~~

**(U) Appendix C:
Agency Implementation Plan Template**

**(U) INSIDER THREAT DETECTION PROGRAM
IMPLEMENTATION PLAN**

(U) References:

- A. White House Memorandum on *Compliance with President's Insider Threat Policy*, dated 19 July 2013
- B. White House Memorandum on *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs*, dated 21 November 2012
- C. Executive Order 13587 *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011
- D. Executive Order 13556 *Controlled Unclassified Information*, 4 November 2010
- E. Executive Order 13526 *Classified National Security Information*, 29 December 2009
- F. White House Memorandum on *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, dated 23 August 1996
- G. *Section 811 of the Intelligence Authorization Act for FY 1995*
- H. Presidential Decision Directive/NSC-12 *Security Awareness and Reporting of Foreign Contacts*, 5 August 1993

- I. Executive Order 12333 *United States Intelligence Activities, as amended*, 4 December 1981
- J. Executive Order 10450 *Security Requirements for Government Employment*, 27 April 1953,
- K. (Insert any references related to your agency, especially the statutes that created your agency. Your agency derived many powers in the "charter" legislation or regulations.)

(U) I Objective: By [date], establish an Insider Threat Detection program within (List your department or agency) in accordance with References A through K and within funding and resource allocations.

(U) II Tasks: The following tasks will be completed in order to meet the above objective. The person responsible for the completion of the task is identified next to the task:

- 1. [Title of person responsible] will designate a Senior Official with authority to provide management, accountability and oversight of the organization's insider threat program and make resource recommendations. The Senior Official's duties include:
 - a. 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.
 - b. Providing management and oversight of the insider threat program and provide resource recommendations to the agency head.

UNCLASSIFIED//~~FOUO~~

- c. Developing and promulgating a comprehensive agency insider threat policy to be approved by the agency head by 21 May 2013.
 - d. Submitting to the agency head an implementation plan for establishing an insider threat program.
 - e. Submitting to the agency head an annual report regarding the progress and/or status of the insider threat program.
 - f. Ensuring the insider threat program is developed and implemented in consultation with the Office of General Counsel and civil liberties and privacy officials.
 - g. Oversee the preparation and submission of quarterly Key Information Sharing and Safeguarding Indicators to the Senior Information Sharing and Safeguarding Steering Committee.
 - h. Establishing oversight mechanisms or procedures to ensure proper handling and use of records and data.
 - i. Ensuring access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.
 - j. Ensuring the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order (E.O.) 13587.
 - k. Facilitating oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines.
2. [Title of person responsible] will establish a working group comprised of agency personnel who have equity in this program, i.e. Security, HR, IA, Inspector General, CI, Office of the General Counsel, civil liberties and privacy officials. This group will assist in the development and implementation of this program.
 3. [Title of person responsible] will write insider threat program policy, which will:
 - a. Identify the Senior Official, by name or title, with authority to provide management, accountability and oversight of the organization's insider threat program and make resource recommendations.
 - b. Ensure personnel assigned to the insider threat program are fully trained in:
 - i. Counterintelligence and security fundamentals;
 - ii. Department or agency procedures for conducting insider threat response actions;
 - iii. Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;
 - iv. Applicable civil liberties and privacy laws, regulations and policies;
 - v. 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.
 - c. 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.
 - d. Establish procedures for access requests by insider threat program involving particularly sensitive or protected information.
 - e. 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.
 - f. Ensure insider threat program has timely access, as otherwise permitted, to available U.S.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

g. Ensure insider threat program includes:

- i. 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.
- ii. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.
- iii. 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.
- iv. 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 users.

h. Ensure the insider threat program:

- i. Provides 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.
- ii. Provides insider threat awareness training annually.

iii. Insider Threat awareness training will address current and potential threats in the work and personal environment and shall include, at a minimum, the following topics:

1. The importance of detecting insider threats by cleared employees;
 2. The importance of reporting suspected activity to insider threat personnel;
 3. Methodologies of adversaries to recruit trusted insiders and collect classified information;
 4. Indicators of insider threat behavior and procedures to report such behavior;
 5. Counterintelligence and security reporting requirements.
- iv. Verifies that all cleared employees have completed the required insider threat awareness training.
 - v. Establishes and promotes 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.
 - i. Establish an integrated capability to monitor and audit information for insider threat detection and mitigation.
 - j. Address evaluation of personnel security information.
 - k. Establish and implement employee Insider Threat Awareness training.
 - l. Detail employee reporting responsibility.
 - m. Establish a centralized analysis, reporting and response capability.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- n. Develop and implement sharing policies and procedures:
- i. Counterintelligence
 - ii. Security
 - iii. Information Assurance
 - iv. Human Resources
- o. Address legal, privacy, civil rights and civil liberties issues.
- p. Detail how to perform self assessments of compliance with insider threat policies and standards.
- q. Detail how to report the results of the self assessments to the Senior Information Sharing and Safeguarding Steering Committee.
- r. Detail support to independent assessments.
4. The insider threat program policy will be approved by [Title of person responsible].
5. [Title of your department or agency head] will ensure personnel assigned to the insider threat program are fully trained in:
- a. Counterintelligence and security fundamentals;
 - b. Department or agency procedures for conducting insider threat response actions;
 - c. Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;
 - d. Applicable civil liberties and privacy laws, regulations and policies;
 - e. 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.
6. [Title of your department or agency head] will 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.
7. [Title of your department or agency head] will establish procedures for access requests by the insider threat program involving particularly sensitive or protected information.
8. [Title of your department or agency head] will 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.
9. [Title of your department or agency head] will ensure insider threat program has timely access, as otherwise permitted, to available U.S. Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.
10. [Title of your department or agency head] will ensure insider threat program includes:
- a. 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.
 - b. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.
 - c. 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.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

- d. Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful U.S. Government authorized purposes and can result in criminal or administrative actions against the users.
11. [Title of your department or agency head] will ensure the insider threat program:
- a. Provides 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.
 - b. Provides insider threat awareness training annually.
 - c. Includes in the insider threat awareness training the current and potential threats in the work and personal environment and shall include, at a minimum, the following topics:
 - i. The importance of detecting insider threats by cleared employees;
 - ii. The importance of reporting suspected activity to insider threat personnel;
 - iii. Methodologies of adversaries to recruit trusted insiders and collect classified information;
 - iv. Indicators of insider threat behavior and procedures to report such behavior;
 - v. Counterintelligence and security reporting requirements.
 - d. Verifies that all cleared employees have completed the required insider threat awareness training.
 - e. Establishes and promotes 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.
 - f. Establishes oversight mechanisms or procedures to ensure proper handling and use of records and data.
 - g. Ensures access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.
 - h. Ensures the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by E.O. 13587.
 - i. Facilitates oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines.
12. [Title of person responsible] will establish an integrated capability to monitor and audit information for insider threat detection and mitigation.
13. [Title of person responsible] will establish and implement employee Insider Threat Awareness training.
14. [Title of person responsible] will establish a centralized analysis, reporting and response capability.
- (U) **III Time Allocation:** Each task will be completed on the date indicated:
1. Designate a Senior Official(s) with authority to provide management, accountability and oversight of the organization's insider threat program and make resource recommendations in accordance with minimum standards, complete dd-mmm-yyyy.

UNCLASSIFIED//~~FOUO~~

2. Establish a working group comprised of agency personnel who have equity in this program, i.e. Security, HR, IA, Inspector General, Counterintelligence, Office of the General Counsel, civil liberties and privacy officials, complete by dd-mmm-yyyy.
3. Write insider threat program policy in accordance with References A through J, complete by dd-mmm-yyyy.
4. Approve insider threat program policy, complete by dd-mmm-yyyy.
5. Hire or train insider threat personnel to minimum standards, complete by dd-mmm-yyyy.
6. Develop, 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, complete by dd-mmm-yyyy.
7. Develop agreements to be 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, complete by dd-mmm-yyyy.
8. Develop and deploy classified and unclassified network banners informing users that their activity on the network is being monitored for lawful U.S.

- States Government authorized purposes and can result in criminal or administrative actions against the users, complete by dd-mmm-yyyy.
9. Develop an insider threat awareness training program to minimum standards, complete dd-mmm-yyyy.
10. Develop a method to verify that all cleared employees have completed the required insider threat awareness training, complete by dd-mmm-yyyy.
11. Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, complete by dd-mmm-yyyy.
12. Establish an integrated capability to monitor and audit information for insider threat detection and mitigation, complete by dd-mmm-yyyy.
13. Establish a centralized analysis, reporting and response capability, complete by dd-mmm-yyyy.

(U) **IV Progress:** The individuals identified in the Tasks paragraphs are responsible for reporting on a weekly basis the status and completion percentage of each task. If there are delays detail the delays and the recommended solutions.

UNCLASSIFIED//~~FOUO~~

(U) Appendix D: Insider Threat Priority Area Questionnaire

(U) Executive Order 13587 *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* creates new requirements for self- and independent assessments of the security status of Federal classified networks. To address these responsibilities, the Classified Information Sharing and Safeguarding Office (CISSO), at the direction of the Steering Committee, developed a set of Key Information Sharing and Safeguarding Indicators (KISSIs) and issued a basic reporting tool. KISSI questions were developed, and subsequently improved, through a collaborative inter-agency review process. The data is collected from agencies on a quarterly basis and is used to establish a comprehensive federal baseline of capabilities to share and safeguard classified information. The results are intended to highlight both government-wide and agency specific strengths and weaknesses, thereby enabling prioritized response strategies and technical implementations. The quarterly KISSI reporting mechanism is meant to serve as an assessment tool to track progress. Questions related to an agency's insider threat posture will be used as a reference point in any subsequent comprehensive independent assessments.

(U) The agency implementation plan should identify the specific office responsible for compiling and submitting KISSI information.

(U) Below is a list of the KISSI questions dealing with insider threat, extracted from the KISSI manual (request a copy of the KISSI manual via e-mail at (b)(3) (classified) or (b)(3) (unclassified)):

15.1 Have we implemented an insider threat program?



(U) Key Information Sharing and Safeguarding Indicators (KISSI)

- A quarterly reporting requirement established under Executive Order (E.O.) 13587 *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* for all agencies.
- Focus on five priority areas under E.O. 13587.
- One priority focus area is insider threat.
- Insider threat KISSI responses should be prepared by Insider Threat Program, with collaboration from across the agency, as appropriate, and approval by the Senior Official.
- Provides an excellent self-assessment window:
 - Has Senior Official been designated?
 - Insider threat policy approved?
 - Program Implementation Plan developed?
 - Program established?
 - General Counsel consultation?
 - Resources allocated?
 - Oversight mechanisms in place?
 - Program access to information established?
 - Documentation of insider threat matters?
 - Records retention rules in place?
 - Centralized analysis in place?
 - Centralized response mechanism in place?
 - Awareness training in place?
 - User monitoring capability in place?
 - Service level agreements in place?
 - Computer monitoring banners implemented?
 - Monitoring consent forms signed?
 - Training for Insider Threat Program personnel?

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

15.2 Have we designated in writing a Senior Official(s) to be responsible for insider threat program efforts?

15.3 Do “insider threat program” accomplishments account for a portion of the designated Senior Official’s written annual performance?

15.4 Are insider threat program requirements fully documented?

15.4.1 Do we have an insider threat policy?

15.4.2 Was the insider threat policy approved by the Agency’s senior executive leadership?

15.4.3 Does Agency policy establish a centralized insider threat program “hub(s)” fully empowered to gather information from components across the Agency (e.g., security, counterintelligence, information assurance, Inspector General, human resources, law enforcement) when that information is deemed necessary by hub personnel for insider threat analysis and response?

15.4.4 Does the insider threat policy ensure legal authorities and civil rights/privacy concerns are addressed in regard to hub operations?

15.4.5 Does the insider threat policy establish written standards for Agency components as to what types of potential anomalies and insider threat concerns must be reported to the centralized hub?

15.4.6 Does the insider threat policy require hub personnel to have counterintelligence training, to include familiarity with “Section 811” reporting requirements?

15.4.7 Does the insider threat policy include a mechanism to ensure that anomalies and insider threat concerns are resolved or reported to appropriate Agency or outside entities in a secure and timely manner?

15.5 Is there a periodic self-inspection process to gauge the effectiveness and efficiency of the insider threat program and correct its shortcomings?

15.6 Is there a written process that involves stakeholders across the Agency to identify and assess risks to critical assets from malicious insiders?

15.7 Does every classified system used by the Agency display a warning banner informing users that their computer activities are subject to monitoring and could be used as a basis to take administrative or criminal action against them?

15.8 Do we have network capabilities to help identify insider threats?

15.8.1 Do we monitor user activities on classified networks for anomalous or suspicious insider behaviors?

15.8.2 Are insider threat-trained personnel conducting analyses on these network user anomalies/behaviors in support of the insider threat hub?

15.8.3 Are insider threat automated “triggers” employed as part of the Agency user monitoring?

15.8.4 Are the insider threat automated triggers regularly reviewed and updated by insider threat program personnel?

15.8.5 Is there adequate compartmentation to ensure insider threat technical tools, procedures, and reporting are secure?

15.9 Is our CIO responsible for the security of all classified systems to which the Agency has access?

15.10 Do our employees access classified IT systems provided by another Agency service provider?

15.10.1 Is there a written document (e.g., Service-Level Agreement (SLA), Memorandum of Agreement (MoA), or Memorandum of Understanding (MoU) that describes how Subscriber will operate external Agency’s classified IT systems (e.g. address services, how it will operate, priorities, responsibilities of involved parties, guarantees and warranties)?

UNCLASSIFIED//~~FOUO~~

15.10.2 Does SLA, MoA, or MoU detail how the external Agency will provide insider threat user monitoring and reporting to support our insider threat program?

15.11 Do we conduct insider threat awareness training?

15.11.1 Is insider threat awareness training for employees conducted at least on an annual basis?

15.11.2 Is insider threat awareness training mandatory for employees with security clearances?

15.11.3 Does insider threat awareness training explain the indicators of insider threat behavior and the importance of insider threat reporting?

15.11.4 Does the insider threat awareness training explain proper procedures for employees to report suspected insider threat activities?

15.11.5 Is insider threat awareness training a mandatory component in orientation programs for all new employees with security clearances?

15.11.6 Is there a system or method for tracking which cleared employees have completed insider threat awareness training?

15.11.7 Does our Agency's senior leadership personally promote insider threat awareness through e-mails, videos, or other outreach techniques using their names or images?

15.11.8 Does our Agency have a publicized internal website providing insider threat case examples, explaining insider threat indicators, and outlining correct reporting procedures?

15.11.9 Are our Human Resources personnel specifically trained on what matters to refer to insider threat personnel?

15.12 Do we have a Security program?

15.12.1 Does our Security program comprise of personnel security, physical security, and information security components?

15.12.2 Does our Agency employ polygraph examinations to assess eligibility for access to classified information?

15.12.3 Does our Agency have a Security Financial Disclosure program?

15.12.4 Are security clearance adjudicators, security officers, and polygraphers trained on what matters to refer to insider threat personnel?

15.12.5 Are insider threat personnel granted access to Agency security program databases for analysis?

15.13 Do we have a foreign travel program?

15.13.1 Is foreign travel reporting required by Security for personal travel of all cleared employees?

15.13.2 Is the foreign travel reporting program required by Security for official travel of all cleared employees?

15.13.3 Are security briefings conducted for travel to countries assessed to be high-risk intelligence for security threats?

15.13.4 Are debriefs conducted for travel to countries assessed to be high-risk intelligence or security threats?

15.14 Do we have a foreign contact reporting program for employees with security clearances?

15.15 Do we use counterintelligence (CI) capabilities?

15.15.1 Does our Agency have a CI program?

15.15.2 Is the CI program implemented through written policies and procedures?

15.15.3 Does the CI program provide analysis and assistance to support our insider threat program?

15.16 Is behavioral science expertise used by insider threat personnel for insider threat deterrence, detection and/or disruption?

(U) Appendix E:
811 Referral Template

(U) This form is Unclassified.

**Espionage/Counterintelligence Referral to the
Federal Bureau of Investigation**




For reporting espionage/counterintelligence allegations and/or suspicions (such as classified information being provided to a foreign power). This includes mandatory Section 811 referrals under the requirements of the Intelligence Authorization Act of 1995. See also 50 USC 402(c). Provide below information in writing to: FBI Counterespionage Section (CD-4), 935 Pennsylvania Ave NW, Washington, DC, 20535. For questions, please call 202-324-4566.



Your Information:	
Name and title:	Date:
Phone (open/secure):	
Email:	
Agency:	
Address:	
Person(s) Involved / Information at Risk:	
Name of person(s) involved:	Position/Job:
Location where suspicious activity/incident occurred:	Date(s)/Time(s):
Is suspicious activity ongoing?	
Does the person suspect he/she may be under scrutiny?	
Classification of information at risk:	
Is SCI material involved?	
Suspicious Activity/Incident Summary:	
Detail the suspicious activity/incident necessitating this referral. If you include classified information, ensure this document and any attachments are appropriately classified:	

• (b)(7)(E)



(U) Appendix F:
Insider Threat Classification Guide
(to be published)

(U) Notes

[Redacted text block containing multiple paragraphs of information, including names, dates, and organizational affiliations. The text is obscured by white rectangular redaction boxes.]

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~



UNCLASSIFIED//~~FOUO~~