U.S. Department of Energy
Washington, DC

ORDER

DOE O 470.5A

Approved 12-06-2024

SUBJECT: INSIDER THREAT PROGRAM

---

1. PURPOSE. To further improve a central Insider Threat Program (ITP) framework to deter, detect, analyze, respond to, and mitigate insider threat actions (such as espionage, sabotage, unauthorized disclosure, workplace violence, etc.) by Department of Energy (DOE) federal and contractor employees.

2. CANCELLATION. This Order cancels DOE Order (O) 470.5, *Insider Threat Program*, June 2, 2014. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive.

3. APPLICABILITY. The ITP applies to all programs to address threats to Departmental assets to include personnel, facilities, material, equipment, information and other DOE or other U.S. government assets.

   a. Departmental Elements.

      (1) Except as otherwise indicated in this section, the requirements in this Order apply to all Departmental elements.

      (2) The Administrator of the National Nuclear Security Administration (NNSA) must ensure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 50 United States Code (U.S.C.) 2402(d) to establish Administration-specific policies, unless disapproved by the Secretary. Any direction to the NNSA will be provided consistent with 50 U.S.C. § 2410.

      (3) The requirements in this Order apply to DOE (and DOE contractor) activities and facilities that are subject to licensing and related regulatory authority or certification by the Nuclear Regulatory Commission (NRC). The requirements in this Order should be applied consistent with Executive Order 12829, *"Executive National Industrial Security Program"* (January 6, 1993); the 1996 *"Memorandum of Understanding Between the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission Under the Provisions of the National Industrial Security Program,"* as may be amended or superseded; and related memoranda of understanding between NRC and DOE concerning classified information, executed in accordance with applicable laws, regulations, policies, directives, and requirements.

b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the Contractor Requirements Document (CRD) (Attachment 1) sets forth requirements of this Order that will apply to contracts that include the CRD.

The CRD must be included in all Management and Operating (M&O) contracts; non-M&O major site/facility contracts; and other non-M&O contracts as determined by the Head of Departmental Element(s) that involve cleared and/or uncleared employees, classified and/or sensitive unclassified information or matter, Special Nuclear Material, nuclear weapons or parts, or contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements.*

c. Equivalencies/Exemptions for DOE O 470.5A. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1 (current version), Departmental Directives Program.

(1) Equivalencies or exemptions from the requirements in this Order must be supported by sufficient analysis to form the basis for an informed risk management decision. The analysis must identify compensatory measures, if applicable, or alternative controls to be implemented.

(2) All approved equivalencies and exemptions under this Order must be entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security or other plan(s). Approved equivalencies and exemptions become a valid basis for operation when they have been entered in SSIMS and documented in the appropriate plan, and they must be incorporated into local procedures at that time.

(3) Many DOE ITP requirements are found in, or based on, regulations issued by federal agencies, and codified in the Code of Federal Regulations (CFR) or other authorities, such as Executive Orders or Presidential Directives. In such cases, the process for deviating from those requirements found in the source document must be applied. If the source document does not include a deviation process, the DOE Office of the General Counsel, or if an NNSA element is involved, the NNSA Office of the General Counsel must be consulted to determine whether and how deviation from the source can be legally pursued.

(4) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 U.S.C. sections 2406 and 2511, and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this directive for activities under the Director’s cognizance, as deemed appropriate.

4. REQUIREMENTS.

a. Implementation.

(1) Full implementation of the Order must be completed within 180 days.

(2) If compliance cannot be accomplished within 180 days, an implementation schedule must be submitted to the appropriate Head of Departmental Element (or their designee), prior to the deadline stated in (1) above.

(3) Documentation must include timelines and resources needed to fully implement this Order as well as a description of the vulnerabilities and impacts created by delayed implementation of the requirements.

b. ITP. The ITP must include:

(1) A Designated Senior Official (DSO) appointed by the Secretary of Energy.

(2) An Executive Steering Committee (ESC) comprised of designated federal senior leadership to provide oversight of the Department's ITP.

(3) Administrative and functional offices to include, but not limited to, Heads of Departmental Elements and Heads of Field Elements.

(4) Operational Offices, to include but not limited to,

(a) Office of Insider Threat Policy and Assistance (OITPA) as the Insider Threat Program Management Office,

(b) Analysis and Referral Center (ARC) as the hub, an operational entity to conduct centralized information and integration and analysis, and user activity monitoring,

(c) Local Insider Threat Working Groups (LITWGs). LITWGs must:

1 Coordinate and track insider threat response actions to effectively mitigate or eliminate identified insider threats.

2 Ensure all LITWG participants have received training on basic counterintelligence (CI) and security fundamentals, *Section 811 of the Intelligence Authorization Act for FY1995* (Title 50 United States Code (U.S.C.) 402(a)) referral responsibilities via IN, and privacy and civil liberties; and maintain records of such training.

3 Maintain awareness of factors affecting the risk from insider threats.

4 Facilitate access to local data to support the ARC's analytic responsibilities.

5 Refer identified insider threat concerns to the appropriate site stakeholders or DOE Headquarters (HQ) office for action and mitigation in accordance with that office's authorities and capabilities.

6 Ensure the Head of Field Element or their designee, is notified, as appropriate, by LITWG Chairpersons regarding identified/potential insider threats. For DOE HQ facilities, the Office of Headquarters Security Operations (EHSS-40) has the responsibilities for Heads of Field Elements.

7 Ensure Senior Counterintelligence Officers (SCIOs) facilitate information sharing with LITWG Chairpersons or their designee on CI-related ITP matters for situational awareness and oversight purposes, as necessary.

8 Develop and maintain a collaborative environment to identify, coordinate, communicate, and integrate local insider threat activities.

9 Conduct inquiries, gather information, and request findings from any entity authorized to conduct inquiries and investigations relevant to the threat being assessed.

10 Coordinate, synchronize, track, and deconflict actions associated with potential insider threat issues among LITWG action entities (e.g., CI, the Cognizant Security Office [CSO], information assurance [to include cybersecurity] or Office of the Chief Information Officer [OCIO], human capital, etc.) regardless of whether the issues originated locally or from ARC referrals. The LITWG is not intended to replace existing reporting requirements but is a mechanism to ensure collaboration among other programs and organizations that share responsibility and authority to mitigate concerns.

11 Ensure any legal, privacy, civil rights, civil liberties issues are appropriately addressed.

12 At a minimum, each LITWG must include the following core members:

a Head of Field Element or their delegate, as appropriate

b Officially Designated Federal Security Authority(ies) (ODFSA), or their designee

c Chairperson (either a federal or contractor employee) appointed in writing by the Head of Field Element

d SCIO or their designee

e Human Capital representative

f Physical Security representative

g Cybersecurity representative and/or Information Technology representative

h Personnel Security representative.

13 Based upon the needs, structure, and mission of the site, LITWGs may also include representatives of the Offices of General Counsel, Inspector General, and Privacy personnel on either a permanent or *ad hoc* basis.

14 Ensure LITWG members share relevant ITP information among the core members when it is reported to them.

(5) Dedicated ITP personnel.

(a) ITP personnel, per the Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, must be provided continuing education and training in the following areas:

1 CI and security fundamentals

2 conducting response actions

3 gathering, integration, retention, safeguarding, and use of records and data

4 applicable civil liberty and privacy laws

5 Section 811 (Title 50 United States Code (U.S.C.) 402(a)) referral requirements and other applicable policy or statutory investigative referral requirements

(6) The ability to identify insider threats and allow appropriate personnel to take actions to deter, detect, and mitigate insider threats to prevent damage

to DOE facilities, personnel, resources, and capabilities, as well as U.S. national security.

(7) Procedures to ensure ITP information are created, collected, retained, and disposed of in accordance with appropriate laws and guidelines set forth by the National Archives and Records Administration (NARA).

(8) Implementation of the Presidentially-mandated *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,* as referenced in 6.q. of this Order.

c. Employee Training and Awareness.

(1) The ITP must ensure initial and annual workforce awareness training is developed and provided.

(2) Training must be compliant with National Insider Threat Policy requirements and/or 32 CFR Part 2004.

d. Access to Information. The ITP must identify, collect, and process data required to identify and address insider threats.

(1) The ITP requires access to information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following: CI, human capital, security, personnel security, and cybersecurity.

(2) DOE sites, facilities, programs, and personnel must provide, or provide access to, data as required for the ITP to successfully execute its mission.

(3) The ITP must have an electronic records management system.

(4) The ITP must manage all ITP records in accordance with their NARA approved records schedules.

(a) All federal records must be managed in fully electronic format and managed to the records schedules electronically within a system.

(5) The ITP must share relevant ITP information to support a comprehensive risk management framework.

e. User Activity Monitoring (UAM). User activity monitoring must be conducted on national security systems (NSSs), to include classified systems, and where feasible unclassified and other information systems.

(1) The ITP must:

(a) Monitor activity on unclassified networks, when deemed appropriate by the DSO and in coordination with OCIO.

(b) Implement DOE information system usage banners, policies, and user agreements in accordance with OCIO-approved policies.

f. Information Integration, Analysis, and Response.

(1) Data sources and format(s) needed to support the ARC must be documented.

(2) The ITP must:

(a) Include a process to perform information integration, analysis, and response (IAR), which will be coordinated between two operational entities: the LITWGs and the ARC.

(b) Coordinate insider threat analysis, response, and mitigation actions with appropriate law enforcement agencies, Office of Intelligence and Counterintelligence (IN), security, legal counsel, personnel security, Inspector General, human capital, and other cognizant organizations.

(c) Maintain a centralized reporting, analysis, monitoring, and data retention center designated as the ARC.

(d) Establish reportable thresholds (see Attachment 3).

(e) Establish procedures to receive and communicate ITP issues between the LITWG and the ARC and other stakeholders as required.

(f) Ensure IN has the right of first refusal to determine if CI issues exist. CI matters will remain in IN channels with requisite LITWG cognizance for situational awareness purposes.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Ensures, as a Cognizant Security Agency (CSA), DOE maintains an effective ITP in accordance with Executive Order 13587, 32 CFR Part 2004, 32 CFR Part 117, and other national directives and policies.

(2) Appoints the DSO to implement the ITP and lead the Executive Steering Committee.

b. DOE Insider Threat Program.

(1) Designated Senior Official. The DSO must ensure the following:

(a) The ITP has:

1 Head of Departmental Element-identified resources to support the ITP.

2 Personnel who have been assigned insider threat functional duties (OITPA, ARC, LITWGs, functional offices, etc.) and have the proper training and resources.

(b) Implements a comprehensive DOE ITP, consistent with Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, and other national directives and DOE requirements.

1 The ITP is maintained and operated in accordance with applicable laws, privacy, civil liberties, and whistleblower protection requirements.

(c) Maintains a centralized reporting, analysis, monitoring, and data retention capability called the Analysis and Referral Center (ARC) in coordination with DOE-IN to manually and/or electronically gather, integrate, review, assess, and respond to information derived from CI, Security, information assurance, human capital, law enforcement, the monitoring of user activity, and other sources as necessary and appropriate.

(d) Provides the ITP Annual Report to the Secretary of Energy to document and report the progress/status of DOE ITP accomplishments, resource requirements, insider threat risks, program impediments or challenges, and recommendations for program improvements.

(e) Ensures ITP reviews are conducted for compliance with insider threat policy requirements.

1 Periodicity and the level of the review is under the purview of the DSO.

2 Assigns officials to ensure regular oversight reviews are conducted to validate compliance with insider threat policy

guidelines, as well as applicable legal, privacy, and civil liberties protections.

(f) Ensures the OITPA maintains an ITP web page with insider threat resources and reporting instructions accessible by all DOE personnel.

(g) Provides management, accountability, direction, and oversight of the DOE ITP and makes resource/budgetary recommendations to the Secretary of Energy.

1 Establishes and ensures the OITPA, as the Program Management Office for the ITP, assists with the execution of the DSO's responsibilities, to include but not limited to, policy, training, awareness, drafting the annual report and conducting internal and external outreach.

(h) Chairs the Executive Steering Committee (ESC).

(i) Ensures proper handling and use of records and data.

1 Access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.

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

(j) Ensures the ITP receives relevant information, such as CI, security, personnel security, cybersecurity, and human capital.

1 Procedures are established for ITP personnel to have access to information, including classified and Controlled Unclassified Information (CUI), consistent with the LITWG members' clearance levels.

2 Reporting guidelines are established for Departmental Elements to refer relevant insider threat information.

3 The ITP facilitates access to intelligence, CI reporting, and analytical products pertaining to threats to DOE.

(k) Provides, in coordination with the IN Director, direction and oversight for a single and centralized ARC to ensure access to information.

(2) Office of Insider Threat Policy and Assistance (EHSS-OITPA).

(a) Establishes and maintains annual awareness and new employee onboarding ITP training in coordination with Program and Field Elements for implementation.

(b) Establishes, executes, and maintains an ITP awareness campaign and conducts internal and external outreach.

(c) Develops, reviews, and coordinates, in coordination with the ARC, implementation of ITP policies and procedures.

(d) Advises and reports on program effectiveness to the DSO.

1 Provides other support and recommendations to the DSO as needed.

(e) Develops, coordinates with ITP stakeholders, reviews and submits the ITP Annual Report.

(f) Provides, in coordination with the ARC, policy or other guidance and recommendations to Heads of Departmental Elements.

(g) Establishes and maintains an ITP web page with insider threat resources and reporting instructions accessible by all DOE personnel.

(h) Serves as support and provides ITP informational materials and resources to Programs and Field Elements.

(3) Analysis and Referral Center (IN-ARC). As the Department's ITP Hub:

(a) Conducts UAM on all enterprise connected NSS, approves UAM solutions on non-enterprise connected NSS, and integrates non-ARC UAM findings, in accordance with established procedures by the Intelligence Community (IC) and the Executive Agent for Safeguarding Classified Information on Computer Networks or any superseding authority.

1 Ensures UAM is conducted on classified systems with enterprise connectivity and integrates UAM findings from classified systems with no enterprise connectivity.

(b) Collects, compiles, integrates, assesses, and retains DOE enterprise-wide insider threat data in accordance with National Archives and Records Administration (NARA).

1 Maintains information about all referrals per an approved DOE records schedule to enable reviews of ARC analytic performance and to support future searches of historical ARC referrals.

2 Maintains the ITP information in a secure data storage system in accordance with the Privacy Act System of Record.

3 Maintains procedures to ensure ITP information is created, collected, retained, and disposed of in accordance with appropriate laws and guidelines set forth by NARA.

(c) Develops and implements DSO-approved procedures for monitoring enterprise connected classified and DOE enterprise connected unclassified networks for activities indicative of insider threat behavior.

1 Provides guidance for monitoring non-enterprise connected classified networks and assists in the development of procedures for monitoring DOE affiliated unclassified networks.

(d) Develops and implements procedures related to the collection, integration, and analysis of information derived from user activity monitoring tools and software; LITWGs, CI, security, personnel security, cybersecurity, human capital, law enforcement, as well as any other appropriate and legally approved data source.

(e) Notifies, in accordance with DSO-approved procedures, LITWGs, Heads of Departmental Elements, and external entities of suspected or identified insider threat activities and provides operational support in the analysis and mitigation of insider threats as needed.

(f) Creates DSO-approved policies for protecting, interpreting, storing, authorized sharing, and limiting access to user activity monitoring methods and results to include all other ITP information.

(g) Ensures that data, analysis, and other support to the ITP are shared as needed and in accordance with DSO-approved procedures, and in coordination with OITPA.

(h) Identifies and documents data sources and format(s) needed to support the ARC's designated analytic operations.

(i) Reports to the DSO, LITWG Chairperson, and the respective SCIO or others, as appropriate, regarding identified/potential insider threats.

(j) Develops DSO-approved notification procedures, in coordination with OITPA, regarding imminent and routine threats.

(k) Provides recommendations and support to LITWGs regarding mitigation responses to ongoing threat situations and records management.

(l) Provides support to CI, criminal, and administrative investigations, inquiries, and operational activity as required or permitted by law, Executive Order, DOE, Department of Justice, Office of Inspector General, or IC policy.

(m) Maintains liaison internally and externally with insider threat community organizations and hubs to coordinate and share insider threat data and best practices.

c. Executive Steering Committee. The ESC is comprised of designated federal senior leadership from, at a minimum, the Office of Science, the Office of Nuclear Energy, the Office of Environmental Management, the Office of Fossil Energy and Carbon Management, the National Nuclear Security Administration, the Office of Environment, Health, Safety and Security, the Office of Intelligence and Counterintelligence, the Office of the Chief Information Officer, the Office of the General Counsel, and the Office of the Chief Human Capital Officer.

(1) Meets quarterly or as convened by the DSO.

(2) Assesses the ITP's human capital, financial, and technical resource needs.

(3) Reviews the ITP Annual Report before submission to the Secretary of Energy.

(4) Recommends to the Secretary on where resources should be allocated so that the ITP is positioned to achieve the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

(5) Advises the DSO regarding management, direction, guidance, and policy oversight of the ITP.

(6) Serves as advocate for LITWGs and provides materials and facilitates learning across the LITWG Program.

d. Local Insider Threat Working Groups (LITWGs).

(1) Coordinate and track insider threat response actions to effectively mitigate or eliminate identified insider threats.

(a) Report insider threat information to the Head of Field Element, ARC, and appropriate authorities as required.

(b) Report insider threat events to the ARC for trend analysis, case management, and retention purposes, as per Attachment 3.

(c) Provide awareness briefings, program information and other communication to support a robust, effective, and continually updated local security awareness program.

(2) Ensure all LITWG participants have received training on basic CI and security fundamentals, *Section 811 of the Intelligence Authorization Act for FY1995* referral responsibilities via IN, and privacy and civil liberties; and maintain records of such training.

(3) Maintain awareness of factors affecting the risk from insider threats.

(4) Facilitate access to local data to support the ARC's analytic responsibilities.

(5) Refer identified insider threat concerns to the appropriate site stakeholders or DOE HQ office for action and mitigation in accordance with that office's authorities and capabilities.

(a) Coordinate activities to assist local authorities, as assigned by Head of Field Element or NNSA, to ensure that local insider threat data and records are developed, maintained, shared, and protected as required.

(6) LITWG Chairpersons ensure the Head of Field Element or their designee, is notified, as appropriate, regarding identified/potential insider threats.

(7) SCIOs facilitate information sharing with LITWG Chairpersons or their designee on CI-related ITP matters for situational awareness and oversight purposes, as necessary.

(a) Ensure IN has the right of first refusal to determine if CI issues exist. CI matters will remain in IN channels with requisite LITWG cognizance for situational awareness purposes.

(8) Develop and maintain a collaborative environment to identify, coordinate, communicate, and integrate local insider threat activities.

(9) Conduct inquiries, gather information, and request findings from any entity authorized to conduct inquiries and investigations relevant to the threat being assessed.

(10) Coordinate, synchronize, track, and deconflict actions associated with potential insider threat issues among LITWG action entities (e.g., CI, the CSO, information assurance [to include cybersecurity] or OCIO, human capital, etc.) regardless of whether the issues originated locally or from ARC referrals. The LITWG is not intended to replace existing reporting requirements but is a mechanism to ensure collaboration among other programs and organizations that share responsibility and authority to mitigate concerns.

(11) Ensure any legal, privacy, civil rights, civil liberties issues are appropriately addressed.

(12) At a minimum, each LITWG must include the following core members:

(a) Head of Field Element or their delegate, as appropriate

(b) Officially Designated Federal Security Authority(ies) (ODFSA), or their designee

(c) Chairperson (either a federal or contractor employee) appointed in writing by the Head of Field Element

(d) SCIO or their designee

(e) Human Capital representative

(f) Physical Security representative

(g) Cybersecurity representative and/or Information Technology representative

(h) Personnel Security representative.

(13) Based upon the needs, structure, and mission of the site, LITWGs may also include representatives of the Offices of General Counsel, Inspector General, and Privacy personnel on either a permanent or *ad hoc* basis.

(14) Ensure LITWG members share relevant ITP information among the core members when it is reported to them.

(a) The LITWG Chairperson and/or the LITWG federal representative, in conjunction with the LITWG members, evaluate the information and identify action entities. This process ensures LITWG members

with a stake in the matter are aware of the referral or inquiry and work together to address the issue.

(b) Ensure LITWGs establish procedures to receive and communicate ITP issues to the ARC. These procedures:

1 Ensure a Head of Field Element-approved ITP Plan at each site incorporated in the approved Security Plan and Counterintelligence Site Support Plan.

2 Ensure that LITWGs report to the ARC insider threat events as outlined in Attachment 3 of this Order.

3 Ensure LITWGs confirm receipt of ARC referrals and provide updates to the ARC at 30-day intervals until resolved.

4 Ensure activation of the LITWGs in response to a reported insider threat or concern.

5 Evaluate if the reported insider threat presents an immediate threat of serious injury to personnel, critical operations, or loss of sensitive information.

6 Ensure a method to report information to IN, with a subsequent report to the DSO, and Head of Departmental/Field Element, and LITWG Chairperson for issues that have a CI nexus, as outlined in Attachment 3 of this Order.

e. DOE General Counsel. Provides legal advice and assistance to federal employees assigned to the LITWG to support the ongoing operation of the ITP as required.

f. Office of Intelligence and Counterintelligence. The Director or their designee:

(1) Ensures SCIO/CI Field Offices will have the right of first refusal to determine if CI issues exist. CI matters will remain in CI channels with requisite LITWG awareness for situational awareness purposes only.

(2) Reviews, analyzes, and assesses ITP data for indications of CI concerns.

(3) Provides support to the ESC, OITPA, and the ARC.

(4) Establishes and provides guidance to, and develops, DSO-approved requirements for LITWGs.

(5) Provides funding for ARC personnel, technical resources, and facilities to support ITP data collection, analysis, and referral activities.

(6) Implements DOE-IN ARC provided UAM solution on IN NSS that have enterprise connectivity. On IN NSS that do not have enterprise connectivity, a DOE-IN ARC-approved UAM solution must be implemented, and any findings are reported to the DOE-IN ARC, as applicable.

(7) Directs SCIOs to review and provide input to the local ITP Plan.

(8) Ensures that necessary intelligence and CI data, as well as IC threat reporting, are available to, and shared with, the appropriate elements of the ITP.

(a) Directs SCIOs to brief LITWG Chairpersons or their designee on CI-related ITP matters for situational awareness in accordance with the Chairperson or designee's clearance and need to know.

(b) Directs SCIOs to ensure insider threat is included as part of their strategic plans.

(9) Ensures all LITWG participants have received training on basic CI and security fundamentals, *Section 811 of the Intelligence Authorization Act for FY1995* (Title 50 United States Code (U.S.C.) 402(a)) referral responsibilities via IN, and privacy and civil liberties; and maintain records of such training.

g. Office of Environment, Health, Safety and Security. The Director or their designee:

(1) Provides funding for personnel and technical resources to support the OITPA.

(2) Coordinates with the OITPA to provide and receive security-related information.

(3) Reviews insider threat indicators for security relevance.

(4) Provides support to the ESC, OITPA, and ARC.

(5) Ensures that information necessary to conduct an insider threat is shared in a timely manner with the appropriate elements of the ITP as requested.

h. Office of the Chief Information Officer.

(1) Facilitates ITP data collection and user monitoring needs regarding information networks, technology, and systems.

(2) Ensures that all ITP laws, regulations and policies regarding information system user notification, acceptable use, acknowledgement, training, and awareness are satisfied to include UAM, Network User Agreements, and banners.

(3) Provides support to the ESC, OITPA, and ARC.

(4) Provides funding and technical resources to support OCIO-specific ITP activities; NNSA and IN coordinates and provides funding for their respective classified processing responsibilities.

(5) Advises the DSO, OITPA, and ARC regarding ITP record creation, management, and retention requirements.

(6) Coordinates with the ARC to identify and mitigate insider threat vulnerabilities.

(7) Provides guidance and recommendations on information sharing pursuant to the ITP.

(8) Ensures that information necessary to conduct an insider threat analysis is shared in a timely manner with the appropriate elements of the ITP as requested.

i. Chief Privacy Officer.

(1) Provides recommendations and guidance, in cooperation with the DOE Senior Agency Official for Privacy (SAOP), to:

(a) Ensure ITP compliance with the Privacy Act of 1974, including drafting and publishing any required Privacy Act SORNs.

(b) Ensure that the ITP establishes a stand-alone ITP Privacy Act System of Records Notice that provides transparency and documents how information about individuals is collected, used, maintained, and disseminated by the Department for the ITP.

(c) Facilitate application of the Fair Information Practice Principles (FIPPs) and other privacy standards into ITP activities, including data collection, information sharing, and analysis.

(2) Conducts an annual privacy impact assessment of the ITP that identifies potential privacy risks and recommends measures to mitigate those risks.

(3) Participates in the drafting of the ITP Annual Report.

(4) Responds to breaches of Personally Identifiable Information (PII) related to ITP activities as outlined in DOE O 206.1 (current version).

(5) Provides support to the ESC, OITPA, and ARC.

(6) Ensures that information necessary to conduct an insider threat is shared in a timely manner with the appropriate elements of the ITP as requested.

j. Office of the Chief Human Capital Officer.

(1) Ensures identification of, and access to, appropriate data sources to support the needs of the ITP, including, but not limited to, personnel files, travel records, and disciplinary files.

(2) Advises the ESC, DSO, OITPA, and ARC regarding pre-employment screening tools and procedures that may be used to identify and neutralize insider threats.

(3) Ensures that new employee briefings include ITP employee requirements, employee rights, and employee responsibilities.

(4) Provides support to the ESC, OITPA, and ARC.

(5) Provides funding and technical resources to support human capital-specific ITP activities.

(6) Recommends potential actions against federal employee(s) based on human capital procedures.

(7) Ensures that information necessary to conduct an insider threat is shared in a timely manner with the appropriate elements of the ITP as requested.

k. Heads of Departmental Elements.

(1) Comply with the ITP requirements defined in this Order as it relates to establishment of the ITP within the prescribed timeline (Section 4.a), and the establishment, and maintenance of LITWGs.

(2) Submit information to the DSO for the ITP Annual Report.

(3) Ensure oversight, governance, resources, and funding are provided to their respective LITWGs.

(4) Seek and apply funding and technical resources to support ITP activities under their purview and in accordance with DSO needs.

(5) Ensure any legal, privacy, civil rights, civil liberties issues are appropriately addressed.

(6) Ensure that employees report insider threats consistent with their training.

(7) Ensure that all records associated with insider threat data and analyses are developed, maintained, shared, and protected as required by law, federal policy, or DOE regulations.

(8) Ensure all contracting officers are made aware of the requirements of this Order and the accompanying CRD.

(9) Determine other non-M&O contracts for inclusion per this Order's CRD and corresponding to Section 3.b of this Order.

(10) Ensure ITP training is conducted and reported annually as required, to include, but not limited to:

(a) ITP-developed annual Insider Threat Program training (as stated in the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Section I) for the workforce.

(b) Practitioner training.

(c) New Employee Onboarding Training.

(11) Ensure information necessary to conduct an insider threat is shared in a timely manner with the appropriate elements of the ITP as requested.

(12) Implement additional security measures not limited to addressing preventing acts of workplace violence and associated behaviors and serve as a local conduit for reporting by coordinating, when necessary, with the LITWGs, ARC, and OITPA.

l. National Nuclear Security Administration.

(1) In addition to Head of Departmental Elements requirements, National Nuclear Security Administration will have Associate Administrator and Chief for Defense Nuclear Security (NA-70) develop and coordinate NNSA specific policy and guidance and is responsible for implementation of this Order.

(2) Provides functional management support to NNSA in implementing the ITP.

(3) Implements an NNSA enterprise capability to conduct analysis, oversight, risk mitigation, and reporting of unauthorized disclosures of NNSA information.

(4) Implements DOE-IN ARC provided UAM solution on NNSA NSS that have enterprise connectivity. On NNSA NSS that do not have enterprise connectivity, a DOE-IN ARC-approved UAM solution must be implemented, and any findings are reported to the DOE-IN ARC as applicable.

m. Heads of Field Elements.

(1) Within 120 days of the publication of this Order, identify and provide the names and contact information of the LITWG Chairperson and Co-Chairperson, as appropriate, to the Head of the Departmental Element, the DSO, OITPA, and the ARC.

(a) Appoint a federal representative to establish a LITWG within 60 days of the publication of this Order.

(2) Implement all requirements as defined in this Order and approved and documented in the local approved ITP Plan.

(a) Coordinate the ITP Plan with all local ITP stakeholders.

(3) Submit budget requirements to the Head of Departmental Element for assigned ITPs.

(4) Submit information to the Head of Departmental Element for the ITP Annual Report.

(5) Ensure insider threat data, records, and analyses developed, maintained, and shared, are protected as required by law, federal policy, or DOE regulations.

(6) Ensure that all employees are aware of individual and organizational ITP requirements and responsibilities.

(7) Ensure any legal, privacy, civil rights, civil liberties issues are appropriately addressed.

(8) Provide direction to all contractors regarding ITP requirements and responsibilities in accordance with applicable contract requirements.

(9) Ensure employees have received the ITP-developed initial and annual ITP training (as stated in the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Section I) and awareness and report results to the DSO.

(10) Ensure that employees report insider threats consistent with their training.

(11) Work with appropriate offices to confirm and ensure all authorized contractor personnel are in compliance with ITP requirements in the CRD.

(12) Notify contracting officers of affected contracts that must include the CRD.

(13) Ensure information necessary to conduct an insider threat is shared in a timely manner with the appropriate elements of the ITP as requested.

n. ITP Personnel.

(1) Ensure implementation of the Presidentially-mandated *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* as outlined in Reference 6.q.

(2) Be trained in all applicable functional areas of the ITP.

(3) Incorporate insider threat-related policies, procedures, and resources from CI, security, human capital, legal counsel, personnel security, information assurance (to include cybersecurity), and other DOE elements that contribute to deterring, identifying, and mitigating insider threats.

o. Contracting Officers. Ensure the CRD (Attachment 1) of this Order is incorporated into affected contracts via the Laws, Regulations, and DOE Directives clause of the contracts.

(1) Incorporation must occur as soon as possible, but in no event more than 180 days following the issuance of the CRD.

p. DOE Employees.

(1) Ensure completion of mandatory initial and annual ITP training.

(2) Ensure insider threat events are reported consistent with the requirements of this Order.

(a) Ensure insider threat events are reported as articulated in initial and annual ITP training.

(b) Ensure reports involving topics of a sensitive or classified nature are handled through appropriate, approved, and authorized channels.

(3) Cooperate with ITP officials attempting to resolve issues of concern.

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Note: DOE O 251.1, current version, provides a definition for "invoked technical standard."

7. REFERENCES.

a. Public Law 118-31, National Defense Authorization Act for Fiscal Year 2024.

b. Public Law 83-503, Atomic Energy Act of 1954, as amended.

c. 5 U.S.C. 552a, Privacy Act of 1974, as amended.

d. 10 CFR Part 1017, Identification and Protection of Unclassified Controlled Nuclear Information

e. 32 CFR Part 117, National Industrial Security Program Operating Manual.

f. 32 CFR Part 2001, Classified National Security Information.

g. 32 CFR Part 2002, Controlled Unclassified Information.

h. 32 CFR Part 2004, National Industrial Security Program (NISP).

i. Executive Order (E.O.) 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters.

j. E.O. 12333, United States Intelligence Activities, as amended.

k. E.O. 12829, National Industrial Security Program, dated January 6, 1993, as amended.

l. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, dated June 30, 2008, as amended.

m. E.O. 13526, Classified National Security Information, dated December 29, 2009.

n. E.O. 13556, Controlled Unclassified Information, dated November 4, 2010.

o. E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011.

p. Presidential Decision Directive/NSCC-12, Security Awareness and Reporting of Foreign Contacts, dated August 5, 1993.

q. Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, dated November 12, 2012.

r. White House Memorandum on Compliance with President's Insider Threat Policy, dated July 19, 2013.

s. White House Memorandum on Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies, dated August 23, 1996.

t. Secretary of Energy Memorandum, Designating the Department of Energy's Designated Senior Official for Insider Threat and Updating DOE Order 470.5, Insider Threat Program, dated February 7, 2023.

u. Secretary of Energy Memorandum, Establishment of a Department of Energy Insider Threat Program, dated December 9, 2013.

v. CG-ITP-1, DOE Classification Guide for the Insider Threat Program (current version) (CUI).

w. CNSSD-504, Protecting National Security Systems from Insider Threat (current version).

x. DOE O 142.3*, Unclassified Foreign Nationals Access Program* (current version).

y. DOE 205.1, *Department of Energy Cybersecurity Program* (current version).

z. DOE O 206.1, *Department of Energy Privacy Program* (current version).

aa. DOE O 243.1, *Records Management Program* (current version).

bb. DOE O 470.3, *Design Basis Threat* (current version).

cc. DOE O 470.4, *Safeguards and Security Program Planning* (current version).

dd. DOE O 471.1, *Identification and Protection of Unclassified Controlled Nuclear Information* (current version).

ee. DOE O 471.6, *Information Security* (current version).

ff. DOE O 471.7, *Controlled Unclassified Information* (current version).

gg. DOE O 472.2, *Personnel Security* (current version).

hh. DOE O 475.1, *Counterintelligence Program* (current version).

ii. DOE O 475.2, *Identifying Classified Information* (current version).

jj. DOE O 486.1, *Foreign Government Sponsored or Affiliated Activities* (current version).

kk. DOE-STD-1227-2017*, Local Insider Threat Working Group Structure, Roles, and Response Actions* (current version).

8. DEFINITIONS.

a. Assessment. A review, evaluation, inspection, test, check, surveillance, or audit to determine and document whether items, processes, systems, or services meet specified requirements and perform effectively. (DOE O 151.1, current version) (*see also Insider Threat Assessment)*

b. Cleared Employee. An employee who has been properly granted access to classified information.

c. Cognizant Security Agency (CSA). E.O. 12829, sec. 202, designates these agencies as having National Industrial Security Program implementation and security responsibilities for their own agencies (including component agencies) and any entities and non-CSA agencies under their cognizance. The CSAs are the Department of Defense, DOE, NRC, Office of the Director of National Intelligence, and Department of Homeland Security.

d. Counterintelligence Site Support Plan. Support plan tailored and site-specific to address concerns and will be developed in coordination with IN-20 and the local or servicing CI office. Site-specific CI support plans should address the following areas at a minimum: Threat Analysis, Insider Threat, Information Technology, Awareness, Briefing and Debriefing, Investigations and Inquiries, Liaison, Unclassified Foreign Visits and Assignment support, Security support, Support to the CI Evaluation Program, Foreign Travel, and Training.

e. 811 Referral. DOE referrals (including all referrals originating from within NNSA) to the Federal Bureau of Investigation (FBI) pursuant to Section 811 of the Intelligence Authorization Act of 1995 [Title 50 United States Code (U.S.C.) 402(a)].

f. Employee. For the purposes of this Order, according to the definition in the National Insider Threat Policy, specifically, a person, other than the President and Vice President, employed by, 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.

g. Executive Agent for Safeguarding Classified Information on Computer Networks. National Manager for national security systems whose responsibilities include developing effective technical safeguarding policies and standards that address the safeguarding of classified information within national security systems, as well as

the safeguarding of national security systems themselves; and conducting independent assessments of agency compliance with established safeguarding policy and requirements.

h. Fair Information Practice Principles. Based in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," the Fair Information Practice principles (FIPPs) have informed Federal statute and the laws of many U.S. states and foreign nations and have been incorporated in the policies of many organizations around the world. The FIPPs are critical to how the federal government approaches information management, especially information about people. While the precise expression of the FIPPs has varied over time and in different contexts, the FIPPs always retained a consistent set of core principles that are broadly relevant to agencies' information management practices.

i. Heads of Departmental Elements. For the purposes of this Order, Heads of Departmental Elements include the Assistant Secretaries and Program Office Directors reporting to the Secretary either directly or through the Deputy Secretary or Under Secretaries. The NNSA Administrator is the only NNSA Head of the Departmental Element. For the purposes of this Order, Power Marketing Administrators are Heads of their Departmental Elements. Heads of Departmental Elements implement the requirements and responsibilities assigned to them in this Order. The Secretary, Deputy Secretary, and Under Secretaries may also perform these roles at their discretion.

j. Heads of Field Elements. A term that includes operations offices, field offices, site offices, service centers, project management offices, area offices, government-owned government-operated facilities, and regional office of federally staffed laboratories that report directly to a DOE Headquarters office.

k. Information Integration, Analysis, and Response (IAR). IAR are activities to determine the presence of an insider threat, as well as the activities to mitigate the threat. Such an inquiry or investigation can be conducted by CI, Security, Human Capital, LE, IG or Cybersecurity Elements depending on internal policy governing the conduct.

l. Insider. Any person with authorized access to any U.S. government or contractor resource to include personnel, facilities, information, equipment, networks, or systems.

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

DOE includes in its definition of Insider Threat consideration of harm to self or others, assets, information, and facilities.

n. Insider Threat Assessment. An ARC administrative procedure that includes the systematic and lawful gathering and analysis of information to determine if there are enough questionable behaviors and/or activities, indicative of a potential insider threat issue, to warrant a Referral.

o. Insider Threat Hub. A hub is an analysis and data aggregation capability that brings people, tools, and information together to build comprehensive assessments of behaviors indicative of a potential insider threat. DOE refers to ARC as the DOE ITP Hub.

p. Insider Threat Program Personnel. Individuals who provide operational, administrative, or functional support, whether as a primary or as a collateral duty, to deter, detect, and mitigate insider threats, and are trained in relevant disciplines such as counterintelligence, physical security, cybersecurity, law enforcement, and privacy. Within the DOE ITP, Insider Threat Program Personnel include but are not limited to the DSO and members of OITPA, ARC, and LITWGs.

q. Insider Threat Program Plan. An official document that describes the methodologies, implementation, and the use of resources by a facility to protect the facility, its sites, and its assets.

r. Insider Threat Response Action(s). Activities conducted to determine whether certain matters or information indicate the presence of an insider threat, including activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of CI, security, law enforcement, or Inspector General elements depending on statutory authority and internal policies governing the conduct of such in DOE.

s. Investigation. An act or process of examining or searching for facts.

t. Inquiry. The systematic and lawful gathering of information by a LITWG to ascertain whether there is an insider threat following "allegations, complaints, facts, or circumstances (i.e., Indicators) that a current or former full, parttime, or temporary employee or contractor and/or trusted business partner is, was, or may be engaged in actions constituting an Insider threat. Inquiries are conducted to clarify or resolve potential insider threats."

u. National Security System. Any information system (including any telecommunications system) that is used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency where the use or operation involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or is an integral part of a weapon or weapons system. This also encompasses systems used to support military or intelligence missions. Systems that are specifically identified within approved

legislation or executive order and must be kept classified in the interest of national defense or foreign policy are also considered NSS. All U.S. Government classified networks have also been designated as NSS.

v. Personnel Security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information, special nuclear material, or assignment in sensitive positions.

w. Right of First Refusal. Operational term for providing the LITWG's counterintelligence element (typically the local SCIO office) an opportunity to evaluate all insider threat events and incidents for a nexus to counterintelligence or international terrorism concerns, in accordance with DOE O 475.1 (current version). This evaluation shall take place prior to any administrative or other action taken by stakeholder offices, except in exigent circumstances (e.g., those pertaining to possible injury or death; loss of special nuclear material; loss or destruction of DOE or other US Government assets). Specific procedures for this review will be defined locally as part of the LITWG operating procedures.

x. Security. An integrated system of activities, systems, programs, facilities, and policies for the protection of classified matter, controlled unclassified information, nuclear materials, nuclear weapons, nuclear weapon components, and/or the Department's and its contractors' facilities, property, and equipment.

y. Security Plan. All facilities and sites under DOE cognizance must have a security plan that reflects the assets, security interests, approved S&S program implementation at that location and any residual risks associated with operation under the security plan. A full description can be found in DOE O 470.4 (current version).

z. System of Records Notice (SORN). Notice published in the *Federal Register* prior to an agency's collection, maintenance, use, or dissemination of information about an individual.

aa. 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 US Government information in order to detect insider threats and to support authorized investigations. (CNSSD 504)

9. CONTACT. For information about this Order, contact the Office of Environment, Health, Safety and Security at (202) 586-9020.

BY ORDER OF THE SECRETARY OF ENERGY

DAVID M. TURK
Deputy Secretary

ATTACHMENT 1

CONTRACTOR REQUIREMENTS DOCUMENT

DOE O 470.5A, Insider Threat Program

Regardless of the performer of the work, the contractors must comply with the requirements of this Contractor Requirements Document (CRD) and with National Nuclear Security Administration (NNSA) and other Department of Energy (DOE) Heads of Field Element direction. Each contractor is responsible for disseminating the requirements and NNSA or other DOE Heads of Field Element direction to subcontractors at any tier to the extent necessary to ensure the contractors' and subcontractors' compliance with the requirements.

Contractors must provide data, information, systems, and any other support to the DOE Insider Threat Program (ITP) in accordance with applicable laws, regulations, policies, directives, and other requirements as directed through contract by the NNSA or other DOE Heads of Field Element(s).

A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, *Procedural Rules of the Assessment of Civil Penalties for Classified Information Security Violations*.

In addition to the CRD, contractors are responsible for complying with Chapters 1 through 6, Attachment 2, and Attachment 3, to DOE O 470.5A, which provides program requirements and/or information applicable to contracts in which this CRD is inserted.

ATTACHMENT 2

INSIDER THREAT PROGRAM BASELINE REQUIREMENTS

The intent of this Attachment is to establish baseline requirements for all DOE Departmental Elements to provide protection to DOE's assets. This Attachment and all subsequent Chapters (1-6) and Attachment 3 applies to DOE Employees and Contractors.

CHAPTER 1. INSIDER THREAT PROGRAM MANAGEMENT

The purpose of this chapter is to address the management and operations of the overall ITP established at a DOE site or facility. This includes ensuring the site's ITP accounts for all local organizations engaged at a given site, the Local Insider Threat Working Group (LITWG) has the necessary team composition to execute the program, as listed in paragraph 4.b.(4)(c) of this Order and has the supporting plans, procedures, and resources.

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

    a. Implement and manage the operational elements of the ITP for the site(s) under their cognizance.

    b. Identify insider threats and allow appropriate personnel to take actions to deter, detect, and mitigate insider threats to prevent damage to DOE facilities, personnel, resources, and capabilities, as well as U.S. national security.

    c. Ensure an Insider Threat Program Senior Official (ITPSO) is appointed by the Contractor Senior Management Official for entities who have a facility clearance. If the appointed ITPSO is not the contractor Facility Security Officer (FSO), then the ITPSO must ensure the FSO is an integral member of the contractor's ITP in accordance with 32 CFR Part 117.7(b).

    d. Define execution of the ITP for their respective site, to include the considerations of those sites with more complex organizational structures involving multiple Heads of Field Elements, contractors, subcontractors, users, guest researchers, etc. to ensure the scope of the LITWG(s) membership and to ensure communications between the varied entities/organizations. Those in close proximity or the same geographical area must coordinate with each other.

    e. Establish a LITWG that comprises representatives with the authority, expertise, and means to administer an effective program (i.e., perform inquiries and collect data as appropriate), with the understanding that other site specialists can be leveraged to support the LITWG, when necessary, based on the need for specific information on a specific situation and data with a nexus to identify potential insider concerns.

        (1) At a minimum, each LITWG must include the following core members:

            (a) Head of Field Element or their delegate, as appropriate

            (b) Officially Designated Federal Security Authority(ies) (ODFSA), or their designee

            (c) Chairperson (either a federal or contractor employee) appointed in writing by the Head of Field Element

(d) Senior Counterintelligence Officer (SCIO) or their designee

(e) Human Capital representative

(f) Physical Security representative

(g) Cybersecurity representative and/or Information Technology representative

(h) Personnel Security representative.

f. Based upon the needs, structure, and mission of the site, LITWGs may also include representatives of the Offices of General Counsel, Inspector General, and Privacy personnel on either a permanent or *ad hoc* basis.

g. Upon request through the applicable Head of Field Element, support data call requests associated with the Designated Senior Official's (DSO's) annual status report.

h. Ensure the ITP activities and procedures are conducted in accordance with applicable laws, whistleblower protections, and legal, privacy, civil rights, civil liberties issues are appropriately addressed.

i. Establish procedures that address all aspects of their ITP, to include the five main program elements (practitioner training, employee training, access to information, user activity monitoring, and data analysis and integration), and how sensitive employee information is handled to ensure it is restricted to ITP personnel. The procedures must also address communication and the exchange of information with the Analysis and Referral Center (ARC).

j. Incorporate or reference the ITP Plan, approved by the Head of Field Element, and procedures in the approved Security Plan and Counterintelligence (CI) Site Support Plan.

k. Ensure ITP information is created, collected, retained, and disposed of in accordance with appropriate laws and guidelines set forth by the National Archives and Records Administration (NARA).

l. Evaluate their ITP through their Contractor Assurance System and support federal line management in the conduct of federal oversight activities.

CHAPTER 2.
INFORMATION INTEGRATION, ANALYSIS, AND RESPONSE

The purpose of this chapter is to develop and maintain threat analytic and response capabilities to gather, integrate, review, assess, and respond to information derived from CI, security, legal counsel, human capital, federal and local law enforcement agencies, user activity monitoring, and other sources as necessary and appropriate.

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

   a. Implement an Insider Threat Evaluation and Response Capability.

      (1) Implement an insider threat evaluation and response capability to gather, integrate, review, and mitigate insider threats. This must be done in a manner to merge disparate information and differing functional perspectives to view indicators more holistically and move toward a proactive detection strategy. This must also be in alignment with the mission of the ARC.

      (2) Coordinate insider threat analysis, response and mitigation actions with appropriate federal and local law enforcement agencies, intelligence, security, personnel security, legal counsel, human capital, and other cognizant organizations.

      (3) Incorporate insider threat-related policies, procedures, and resources from CI, security, human capital, legal counsel, personnel security, information assurance (to include cybersecurity), and other DOE elements that contribute to deterring, identifying, and mitigating insider threats.

      (4) Coordinate, synchronize, track, and deconflict actions associated with potential insider threat issues among LITWG action entities (e.g., CI, the Cognizant Security Office [CSO], information assurance [to include cybersecurity] or Office of the Chief Information Officer [OCIO], human capital, etc.) regardless of whether the issues originated locally or from ARC referrals. The LITWG is not intended to replace existing reporting requirements but is a mechanism to ensure collaboration among other programs and organizations that share responsibility and authority to mitigate concerns.

      (5) Evaluate if the reported insider threat presents an immediate threat of serious injury to personnel, critical operations, or loss of sensitive information.

      (6) Self-assessments against the requirements of this Order must be incorporated into the contractor's self-assessment schedule. Reference DOE O 470.4 (current version) for the frequency of the self-assessments.

b. Establish Insider Threat Response Procedures.

(1) Ensure activation of the LITWG in response to a reported insider threat or concern.

(2) Refer identified insider threat concerns to the appropriate site stakeholders or DOE Headquarters (HQ) office for action and mitigation in accordance with that office's authorities and capabilities.

(a) LITWG Chairpersons must ensure the Head of Field Element or their designee, is notified, as appropriate, regarding identified/potential insider threats.

(3) Appropriate LITWG personnel must be designated the authority to conduct administrative inquiries and information gathering efforts to determine the nature and scope of an insider threat and to support the threat assessment process.

(4) Establish procedures that are approved by the Head of Field Element to receive and communicate LITWG insider threat concerns (e.g., inquiries, behavioral assessments) to the DOE ARC.

(5) LITWGs must report insider threat concerns to the ARC in coordination with the applicable ITPSO as outlined in Attachment 3 of this Order.

(6) Ensure a method to report information to IN, with a subsequent report to the DSO, and Head of Departmental/Field Element, and LITWG Chairperson for issues that have a CI nexus, as outlined in Attachment 3 of this Order.

(7) LITWG members must share relevant ITP information among the core members when it is reported to them.

(8) The LITWG Chairperson and or the LITWG federal representative, in conjunction with the LITWG members, must evaluate the information and identify action entities. This process must ensure LITWG members with a stake in the matter are aware of the referral or inquiry and work together to address the issue.

(9) LITWGs must confirm receipt of ARC referrals and provide updates to the ARC at 30-day intervals until resolved.

Establish procedures for documenting and tracking each insider threat case reported and response action(s) taken. Documentation pursuant to the LITWG must be reviewed for proper classification of information and handled accordingly.

CHAPTER 3. INSIDER THREAT PROGRAM PERSONNEL

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

   a. Provide initial training in all applicable functional areas to personnel within 12 months of assignment of ITP duties (or as availability permits) in accordance with the Individual Development Plan and functional training availability and annually thereafter, as listed in Section 4.b. of this Order, in the following areas (i.e., Presidentially-mandated *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*):

      (1) CI and security fundamentals to include legal issues;

      (2) Local procedures for establishing and conducting insider threat response actions;

      (3) Laws and regulations regarding the gathering, integration, retention, safeguarding, and use of insider threat records and data;

      (4) Civil liberties and privacy laws, regulations, and policies; and

      (5) *Section 811 of the Intelligence Authorization Act for FY1995* (Title 50 United States Code (U.S.C.) 402(a)).

   b. Have the capability to provide records certifying completion of required ITP training taken by LITWG members, personnel assigned ITP duties, and all DOE federal and contractor employees.

2. TRAINING. Training requirements for DOE federal and contractor employees are outlined in Chapter 6 of this Attachment.

CHAPTER 4. ACCESS TO INFORMATION

The purpose of this chapter is to establish baseline requirements for DOE to ensure designated federal and contractor ITP personnel have access to appropriate information to detect, analyze, and mitigate insider threat matters.

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

   a. Provide insider threat information and supporting activities upon request to DOE officials and the LITWGs including:

      (1) Cooperates with DOE and all federal agencies during official reviews and investigations concerning the protection of DOE assets to include personnel, facilities, material (e.g., special nuclear material, classified information, etc.), information (sensitive unclassified or classified), equipment, and other DOE or other U.S. government assets.

      (2) Provides access to information necessary to analyze and address suspected or known insider threat activity. This information must include, but is not limited to, relevant employment or personnel files, security records, supervisory files, records pertinent to insider threat (e.g., security, cybersecurity, CI, and human capital), and any other records pertaining to an individual under investigation that are in the possession or control of the contractor or located in the contractor's offices.

      (3) Develops procedures, in coordination with the Head of the Field Element and ARC, for access requests involving sensitive or protected information pertaining to insider threat matters.

      (4) SCIOs facilitate information sharing with LITWG Chairpersons or their designee on CI-related ITP matters for situational awareness and oversight purposes, as necessary.

      (5) Ensures IN has the right of first refusal to determine if CI issues exist. CI matters will remain in IN channels with requisite LITWG cognizance for situational awareness purposes.

      (6) Establishes reporting guidelines or have appropriate agreements in place (memoranda of agreement, memoranda of understanding, etc.) to ensure coordination with the LITWG, CI, security, information assurance (to include cybersecurity), human resources, personnel security (Cognizant Personnel Security Officer [CPSO]), and any other organizational components (i.e., ARC, Office of Inspector General, FBI, Office of Intelligence and Counterintelligence [IN]) identified by the Head of the Field Element or the LITWG Chairperson.

(7) Ensures access to U.S. government intelligence and CI reporting information and analytical products pertaining to adversarial threats.

(8) Ensures access to intelligence and CI reporting information and analytical products received from other agencies pertaining to adversarial threats. DOE O 475.1 (current version) identifies IN's responsibility to provide relevant intelligence/CI information necessary to the ITP.

CHAPTER 5. MONITOR USER ACTIVITY ON NETWORKS

The purpose of this chapter is to maintain the integrity and security of network activities by implementing comprehensive monitoring of user activities within network environments. This is essential for the detection, deterrence, and mitigation of insider threats and unauthorized access.

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

   a. Scope and Methodology.

      (1) Employ the DOE-IN ARC provided UAM solution on National Security Systems (NSS) that have enterprise connectivity or a DOE-IN ARC-approved UAM solution on NSS that do not have enterprise connectivity, and any findings reported to the DOE-IN ARC as applicable. UAM will be used to observe and record the activities and actions of user activities on any device accessing or processing information noted above for detecting insider threats and supporting investigations.

      (2) Develop monitoring procedures for NSS systems that are non-enterprise connected, with guidance or assistance from the ARC, that identify key words, indicators, and criteria to be used to confirm and investigate locally reported insider threat vulnerabilities.

   b. Data Protection and Privacy Compliance.

      (1) Handle non-enterprise connected NSS UAM event data in accordance with policies and procedures to restrict access only to those individuals authorized to handle data codified through formal service level agreements (SLAs) or memorandum of understanding (MOU).

      (2) Secure data collected in support of insider threat detection in compliance with federal regulations (e.g., Personally Identifiable Information (PII)) and law enforcement/CI.

      (3) Protect UAM data in accordance with Title 5 U.S.C. (Privacy Act).

   c. Notification and Monitoring.

      (1) In circumstances where non-enterprise connected NSS UAM results in an insider threat concern, the content must be provided to the SCIO, LITWG, and the ARC for resolution, coordination, and response.

      (2) Network banners on unclassified and classified networks must be consistent with OCIO approved policies (e.g., DOE O 205.1 and DOE O 206.1). The banner must be approved by the local site approving authority in consultation with legal counsel.

(3) For monitoring purposes, the UAM solution's capabilities must include at a minimum, key stroke monitoring, capture of full application content (e.g., email, data import, data export), screen capture, and file shadowing for lawful purposes. The UAM must also incorporate the ability to set triggers/alerts based on user activity. Non-enterprise connected NSS UAM triggers must be approved by the local site approving authority in consultation with legal counsel.

CHAPTER 6. EMPLOYEE TRAINING AND AWARENESS

The purpose of this chapter is to provide the DOE ITP training to their cleared and uncleared workforce.

1. GENERAL REQUIREMENTS. Sites must ensure local ITPs:

   a. Provide initial and annual ITP awareness training to all employees (Management and Operating contractors, subcontractors, users, guest researchers, etc., whose engagement is 6 months or longer) within 30 days of initial employment, entry-on-duty, or following the granting of access to classified information and in accordance with the requirements of this Order.

      (1) Training must address current and potential threats in the work and personal environment and will include at a minimum:

         (a) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.

         (b) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems.

         (c) Indicators of insider threat behavior and procedures to report such behavior.

         (d) CI and security reporting requirements, as applicable.

      (2) Use the ITP training module developed by the OITPA.

         (a) The ITP training module may be incorporated into other related training, such as the Comprehensive Briefing for cleared personnel.

      (3) Establish procedures to validate all employees who have completed the initial and annual refresher insider threat training.

      (4) Have the capability, as requested, to provide annual training records to the respective Head of Field Element.

      (5) Promote local procedures for reporting insider threat activity.

      (6) Provide awareness briefings, program information and other communication to support a robust, effective, and continually updated local security awareness program.

   b. Ensure employees cooperate with ITP officials attempting to resolve issues of concern.

ATTACHMENT 3

LITWG REPORTING GUIDELINES

This Attachment provides information and/or requirements associated with DOE O 470.5A, as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.5A) is inserted.

1. GENERAL. LITWGs must report significant and substantiated LITWG insider threat concerns to the ARC, Head of Field Element, and appropriate authorities as required in coordination with the applicable ITPSO if they fall within one or more of the following categories for the purposes of maintaining a DOE-wide central repository of all insider threat data. Reporting to the ARC should be done in addition to, and not in lieu of, the standard reporting requirements of the LITWG, to include security, cyber, human capital, and others. The categories below contain specific examples to help provide context; however, these should not be construed as an exhaustive list of possibilities.

    a. The ARC must maintain the insider threat event reports in a secure, access-controlled case management system and in compliance with data retention requirements.

    b. The event data particulars will align with SORN restrictions, and may be used for additional ARC assessments, enterprise-wide trend and pattern analysis, historical research, or other metrics-related purposes.

2. REPORTING CATEGORIES.

    a. Exigent Threats. Information pertaining to, or indications of, an immediate and serious threat an individual may pose to DOE installations, facilities, personnel, missions, or resources. Immediate and serious threats are defined as those that present a higher-than-normal risk to personal safety, national intelligence, or DOE operations. Any insider threat incidents that involve nuclear or other hazardous radiological, chemical, or biological materials by nature fall into this category. Examples include: workplace violence, sabotage, destruction of critical data, expressing a desire for self-harm or exhibiting signs of a significant mental health crisis.

    b. Allegiance to the United States. Information pertaining to any individual exhibiting questionable allegiance to the United States through words or actions to include involvement in, support of, training to commit, or advocacy of any act, of treason against the United States. Examples include: expressing support for a foreign political power against the United States, advocating for the overthrow of the U.S. government.

    c. Espionage. Information pertaining to any individual suspected to have unauthorized contact with a potential officer or agent of a foreign power. Examples include: undeclared close and continuing contact with a member of a foreign

country, unauthorized or undisclosed support to a foreign government or military, failure to report undue influence by a foreign interest.

d. Terrorism and Extremism. Information pertaining to an individual providing support to, or who is in contact with, known or suspected domestic or international terrorist or extremist individuals, organizations, or groups. Examples include: communicating with foreign terrorist group members, providing financial support to known terrorist organizations.

e. Violent Criminal or Sexual Conduct. The threat, investigation, arrest, indictment, or charging by a federal, state, or local jurisdiction of any individual involving the loss of life or suspected acts of violence including sexual assaults. Examples include: crimes or the threat of crimes involving violence such as homicide, rape, robbery, aggravated assault, etc.; any criminal offense involving the use of weapons or explosives; involvement in human trafficking.

f. Transnational or Organized Criminal Affiliations. Information pertaining to any individual providing support to known or suspected domestic or international criminal organizations or groups engaged in racketeering activities. Examples include: distributing gang recruitment materials, posting pro-gang videos from a work computer. (Reporting requirements applies to individuals with security clearances only; reporting of non-cleared individuals is considered optional.)

g. Significant Financial Irregularities. Information pertaining to significant changes in an individual's financial status, to include both exhibiting sudden unexplained affluence or an individual's inability to repay significant outstanding debts. Examples include: purchasing a new sports car with cash despite being heavily in debt, embezzlement or related fraudulent financial activity, significant omissions in required financial disclosure documents.

h. Unauthorized Disclosure. Information that indicates an individual is knowingly involved in unauthorized disclosure, theft, loss, or compromise of classified, protected, or proprietary information to a foreign power, an agent of foreign power, the media, or any unauthorized recipient. Examples include: unauthorized publication of classified information to broadcast media sources, intentional posting of sensitive or controlled information to unauthorized websites.

i. Misuse of Information Technology. Information pertaining to an individual significantly and deliberately misusing information technology or exhibiting a pattern of negligent noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology. Examples of significant misuse include: hacking of DOE computer networks, circumventing information technology protection mechanisms, unauthorized transfer of digital data.

j. Personal Candor. Information pertaining to deliberate omission, concealment, or falsification of relevant facts from any personnel security investigations, polygraph examinations, or a pattern of behavior that puts the individual's judgment,

trustworthiness, honesty, or willingness to comply with applicable laws and regulations into question. Examples include: repeatedly lying to supervisors regarding work, falsification of official security documentation.

k. Unexplained Personnel Disappearance. Unexplained and otherwise unauthorized disappearance of any individual during regularly scheduled working hours. Examples include: extensive unauthorized absence violations, unauthorized or concerning undeclared travel. (Reporting requirements applies to individuals with security clearances only; reporting of non-cleared individuals is considered optional.)

3. POTENTIAL INDICATORS OF INSIDER THREATS.

a. Engaging in unreported foreign travel and/or maintaining contact with criminal, extremist, or otherwise unreported foreign entities.

b. Involvement in, or ideation of, acts of workplace violence or self-harm, or exhibiting signs of a significant mental health crisis.

c. Committing significant or repeated security or workplace misconduct events.

d. Violating Cybersecurity protocols involving access to restricted or classified data.

e. Involvement in the unauthorized destruction, compromise, duplication, disclosure, or removal of classified or sensitive data.

f. Attempts to physically access unauthorized, secured, or controlled areas.

g. Violating need-to-know policies.

h. Demonstrating significant financial issues (e.g., bankruptcy, liens, or delinquent debts) or unexplained affluence.

i. Engaging in significant and/or uncharacteristic periods of absences without authorized leave.

j. Displaying significant disgruntlement and grievances with co-workers or leadership.

k. Exhibiting continuous lack of honesty or repeated inability to follow laws and regulations.

l. Involvement in the use, distribution, or manufacture of illegal or contraband substances.