U.S. Department of Energy
Washington, DC

ORDER

DOE O 470.5

Approved: 06-02-2014

SUBJECT: INSIDER THREAT PROGRAM

1. PURPOSE. To establish responsibilities and requirements for the Department of Energy (DOE) Insider Threat Program (ITP). The purpose of the ITP is to deter, detect, and mitigate insider threat actions by Federal and contractor employees in accordance with the requirements of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, dated October 7, 2011, the *National Insider Threat Policy* ("National Policy") *and Minimum Standards for Executive Branch Insider Threat Programs* ("Minimum Standards"), dated November 21, 2012, and other government-wide and DOE requirements. The ITP applies to all programs in an integrated manner that may address threats to personnel, facilities, material (e.g., special nuclear material), information, equipment and other DOE or other United States Government assets. This directive establishes a central ITP for DOE. Any conflict with other DOE Directives or requirements should be reported to the Department's senior insider threat official for resolution.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. Departmental Elements.

      (1) Except as otherwise indicated in this section, the requirements in this Order apply to all Departmental Elements. Direction to National Nuclear Security Administration (NNSA) personnel and programs will be effected through the Secretary of Energy, the Deputy Secretary of Energy, or will otherwise comply with the NNSA Act.

      (2) The Administrator of the 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 3212(d) of the NNSA Act ("NNSA Act") (50 United States Code (U.S.C.) § 2402(d)) to establish Administration-specific policies, unless disapproved by the Secretary.

      (3) This Order applies to the Bonneville Power Administration (BPA). The BPA Administrator will assure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA's self-financing, procurement and other statutory authorities.

      (4) 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 contracts that involve cleared employees, classified information or matter, Special Nuclear Material, nuclear weapons or parts, or contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

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

c. Equivalencies/Exemptions for DOE O 470.5. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1C, *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 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 NNSA Office of the General

Counsel if an NNSA element is involved, 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 (February 1, 1982), codified at 50 U.S.C. Sections 2406 and 2511, and to ensure consistency throughout 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. An ITP must be developed and maintained to deter, detect, mitigate, analyze and respond to insider threats.

b. The ITP must:

(1) Fulfill and maintain consistency with the National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs;

(2) Identify insider threats and take appropriate actions to deter them from causing damage to DOE personnel, resources, capabilities and national security commensurate with the potential consequences of the insider threats' access, intent and ability;

(3) Ensure legal, civil and privacy rights and civil liberties are preserved and protected;

(4) Integrate insider threat related policies, procedures and resources across DOE, that include counterintelligence, security, human capital, legal counsel, information management and other DOE Elements that can contribute to deterring, identifying and managing insider threats;

(5) Identify, collect and process data required to identify and address insider threats;

(6) Coordinate insider threat analysis, response and mitigation actions with appropriate law enforcement agencies, DOE intelligence, security, legal counsel, inspector general, human capital and other cognizant organizations;

(7) Establish, maintain and conduct training or awareness activities to ensure all cleared Federal and contractor employees are informed of their responsibilities and provided required information related to the ITP; and

(8) Monitor user activity on classified networks.

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

d. DOE programs must identify the resources to support the ITP and provide this information to the ITP Working Group (ITPWG).

e. Annual progress/status reports must be prepared for the Secretary of Energy through the ITPWG and the Senior Information Sharing and Safeguarding Steering Committee (SISSSC) established by E.O. 13587 to document and report the progress/status of the ITP.

f. DOE information system usage banners, policies and user agreements must be approved according to Designated Senior Official (DSO) direction and in consultation with the Office of the General Counsel.

g. Senior Counterintelligence Officers must ensure that Local Insider Threat Working Groups (LITWG) are established.

h. Documentation pursuant to the ITP must be reviewed for classified and controlled unclassified information and handled accordingly.

i. DSO-approved insider threat detection, assessment and referral criteria and procedures must be documented.

j. Data sources and format(s) needed to support the centralized analytic operations must be documented.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Establishes, directs and maintains an effective ITP in accordance with Executive Order 13587 and other national directives and policies.

(2) Designates the senior official to lead and coordinate the ITP.

(3) Establishes the ITP Executive Steering Committee (ESC).

b. Designated Senior Official (DSO).

(1) Advises and reports directly to the Secretary of Energy and Deputy Secretary of Energy regarding the planning, construct and operation of the ITP.

(2) Provides management, direction, guidance and oversight of the ITP in accordance with Section 3.a. (1) of this order.

(3) Chairs the ESC.

(4) Establishes and provides direction and oversight to ITP multi-organizational or multi-functional groups in accordance with Section 3.a.(1) of this order, including:

(a) The ITPWG to assist the DSO in developing, coordinating and operating the ITP; and

(b) A single centralized insider threat Analysis and Referral Center (ARC) to collect, integrate, review, assess and initiate referrals or appropriate responses based on information from intelligence, counterintelligence, security, information technology, information assurance, human capital, law enforcement and other sources as necessary and appropriate.

(5) Individually, or through DSO delegation to another individual or group:

(a) Ensures the ITP is consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, other national directives and DOE requirements;

(b) Ensures policies and procedures are developed and maintained for the ITP in accordance with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, other national directives and DOE requirements;

(c) Ensures the ITP is developed and operated in accordance with all applicable privacy, civil liberty and whistleblower protection requirements;

(d) Ensures insider threat response actions (investigation, enforcement, etc.) are appropriately documented and completed for ITP purposes;

(e) Integrates all elements of the ITP into an operational capability, which includes resolving conflicts between competing interests;

(f) Ensures policies, procedures and agreements are established to enable appropriate and timely sharing of information, programs and systems to implement and operate the ITP;

(g) Ensures ITP policies and procedures include protecting and appropriately limiting access to analysis procedures, data and results to authorized personnel as required to perform their functions;

(h) Establishes and maintains ITP training and awareness requirements for all DOE employees and contractors;

(i) Ensures personnel assigned to the ITP are fully trained in applicable areas;

(j) Ensures that ITP-generated records and applicable System(s) of Records(s) are developed, maintained, protected and shared by Federal and contractors employees as required;

(k) Facilitates and coordinates oversight reviews of the ITP;

(l) Establishes procedures for insider threat response actions to clarify or resolve insider threat matters;

(m) Establishes a user monitoring capability on classified networks and systems; and

(n) Ensures program personnel have authorized access to insider threat-related information and data from DOE Elements and other agencies.

(6) Provides resource recommendations to the Secretary of Energy.

(7) Ensures that an annual ITP progress/status report is provided to the Secretary of Energy.

(8) Ensures that DOE submits quarterly reports on Key Information Sharing and Safeguarding Indicators (KISSI) to the SISSSC.

c. Executive Steering Committee (ESC).

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

(2) Includes senior management representation from, at a minimum, the Office of Intelligence and Counterintelligence, Office of Environment, Health, Safety and Security, Office of the Chief Information Officer, Office of the Chief Human Capital Officer, Office of the General Counsel and NNSA.

(3) Addresses resource needs of the ITP.

(4) Reviews and concurs with or rejects the annual ITP progress/status report to the Secretary of Energy.

(5) Designates members of the ITPWG from nominations of sponsoring offices.

d. ITP Working Group.

(1) Includes representation as designated by the ESC, including senior staff level representation from, at a minimum, the Office of Intelligence and Counterintelligence, Office of Environment, Health, Safety and Security, Office of the Chief Information Officer, Office of the Chief Human Capital Officer, Office of the General Counsel and NNSA.

(2) Supports the DSO by:

(a) Reviewing implementation of ITP policies and procedures and advising the DSO as to program status;

(b) Recommending actions and resources to improve the ITP; and

(c) Drafting the annual report and providing it to the ESC for review.

(3) Provides a forum to address cross-organizational issues.

(4) Provides other support and recommendations to the DSO as needed.

e. DOE ITP Analysis and Referral Center (ARC).

(1) Develops and documents DSO-approved insider threat detection, assessment and referral criteria and procedures.

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

(3) Gathers, integrates and analyzes information derived from counterintelligence, security, information assurance, human capital, law enforcement, the monitoring of user activity and other sources as necessary and appropriate to identify potential insider threat activity for referral and response.

(4) Develops DSO-approved policies and procedures for protecting and appropriately limiting access to ARC analysis procedures, data and results to authorized personnel as required to perform their functions.

(5) Through the DSO or according to DSO-approved procedures, refers identified and potential insider threat issues to the appropriate program(s) or office(s) that should lead investigation(s) or other response(s).

(6) Recommends to the DSO which DOE or other agencies' program(s) or office(s) should be notified for each identified/potential insider threat.

(7) Requests support from other DOE/NNSA elements as needed to develop recommendations for insider threat response and mitigation actions.

(8) Develops a method(s) to maintain information about all referrals that are performed by the ARC to enable review of ARC analytics performance and to support future searches of historical ARC referrals.

f. Local Insider Threat Working Groups (LITWG).

(1) Develop and maintain a collaborative environment to identify, coordinate, and integrate local activities to address insider threats.

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

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

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

g. DOE General Counsel.

(1) Provides legal advice and assistance to support development and operation of the ITP as required.

(2) Provides legal advice to the DSO, ESC, ITPWG and ARC.

h. Office of Intelligence and Counterintelligence.

(1) Reviews, analyzes and assesses ITP data for indications of counterintelligence concerns.

(2) Participates in the ESC, ITPWG and the ARC.

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

(4) Provides funding and technical resources to support ITP collection and analysis activities.

(5) Provides facilities for the ARC.

i. Office of Environment, Health, Safety and Security.

(1) Coordinates with the ITP to provide and receive security-related information.

(2) Reviews insider threat indicators for security relevance.

(3) Participates in the ESC, ITPWG and ARC.

(4) Provides funding and technical resources to support ITP security concerns.

j. 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.

(3) Participates in the ESC, ITPWG and ARC.

(4) Provides funding and technical resources to support ITP activities.

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

k. 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) Applies and advises the ESC, DSO, ITPWG and ARC regarding pre-employment screening tools and procedures that may be used to identify and eliminate insider threats.

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

(4) Participates in the ESC, ITPWG and ARC.

(5) Provides funding and technical resources to support ITP activities.

(6) Recommends potential sanctions against Federal employee(s) based on human capital procedures.

l. DOE Program and Staff Offices.

(1) Ensure that planning, data, technical, training, analysis, fiscal and other support to the ITP throughout their organizations is provided as needed.

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

(3) Ensure that employee legal, civil and privacy rights are preserved and protected.

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

(5) Ensure that employees report insider threats consistent with the provisions of the ITP.

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

(7) Ensure that local insider threat data and records are developed, maintained, shared and protected as required.

m. National Nuclear Security Administration.

(1) Ensures that planning, data, technical, training, analysis, fiscal and other support to the ITP throughout NNSA is provided as needed.

(2) Ensures that all NNSA employees are aware of individual and organizational ITP requirements and responsibilities as applicable to NNSA elements.

(3) Ensures that NNSA employee legal, civil and privacy rights are preserved and protected.

(4) Provides direction to all NNSA contractors regarding ITP requirements and responsibilities in accordance with applicable contract requirements.

(5) Ensures that NNSA employees report insider threats consistent with the provisions of the ITP.

(6) Notifies NNSA contracting officers of affected NNSA contracts that must include the CRD.

(7) Ensures that local insider threat data and records are developed, maintained, shared and protected as required.

(8) Participates in the ESC, ITPWG and ARC as required.

n. Contracting Officers.

(1) Upon notification by a DOE/NNSA line management official initiating a procurement activity, incorporate ITP CRD(s), requirements or clauses into affected contracts as appropriate.

6. REFERENCES.

a. Executive Order (E.O.) 10450, Security Requirements for Government Employment, dated April 27, 1953, as amended.

b. E.O. 12333, United States Intelligence Activities, as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008).

c. E.O. 12829, National Industrial Security Program, dated January 6, 1993.

d. 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.

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

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

g. 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.

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

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

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

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

l. Privacy Act of 1974, as amended.

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

n. 10 CFR Part 1045, Nuclear Classification and Declassification.

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

p. DOE O 206.1, *Department of Energy Privacy Program*, dated January 16, 2009.

q. DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, dated May 14, 2010.

r. DOE O 452.8, *Control of Nuclear Weapon Data*, dated July 21, 2011.

s. DOE O 457.1A, *Nuclear Counterterrorism*, dated August 26, 2013.

t. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated March 1, 2010.

u. DOE M 471.3, Admin Chng 1, *Manual for Identifying and Protecting Official Use Only Information*, January 13, 2011.

v. DOE Order 471.3, Admin Chng 1, *Identifying and Protecting Official Use Only Information*, dated January 13, 2011.

w. DOE O 471.6 Administrative Change 1, *Information Security*, dated November 23, 2012.

x. DOE 475.1, *Counterintelligence Program*, dated December 10, 2004.

y. DOE O 475.2A, *Identifying Classified Information*, dated February 1, 2011.

z. Intelligence Authorization Act for Fiscal Year 1995.

7. DEFINITIONS.

a. "Cleared Employee" means an employee who has been properly granted access to classified information.

b. "Employee" is defined, 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.

c. "Insider" means any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks or systems.

d. "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 United States through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or

degradation of U.S. Government resources or capabilities."Insider Threat Response Action(s)" means activities conducted to ascertain whether certain matters or information indicates 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 DOE.

8. CONTACT. For information about this Order, contact the Office of Environment, Health, Safety and Security at (301) 903-4642.

BY ORDER OF THE SECRETARY OF ENERGY:

DANIEL B. PONEMAN
Deputy Secretary

ATTACHMENT 1. CONTRACTOR REQUIREMENTS DOCUMENT

Regardless of the performer of the work, the contractors must comply with the requirements of this contractor requirements document and with National Nuclear Security Administration (NNSA) and other Department of Energy (DOE) program office direction approved by the DOE Insider Threat Program Executive Steering Committee and provided through contract. Each contractor is responsible for disseminating the requirements and NNSA or other DOE program office direction to subcontractors at any tier to the extent necessary to ensure the contractor's and subcontractor's compliance with the requirements.

Contractors must provide data, information, systems, and any other support to the DOE Insider Threat Program in accordance with applicable laws, regulations, policies, directives and other requirements as directed through contract by the NNSA or other DOE program office(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*.