U.S. Department of Energy
Washington, DC

ORDER

DOE O 475.3

Approved: 02-23-2026

SUBJECT: MANAGEMENT OF THE DEPARTMENT OF ENERGY INTELLIGENCE ENTERPRISE

1. PURPOSE. Provides for the management of the Department of Energy (DOE) Intelligence Enterprise and assigns responsibilities for DOE's intelligence and counterintelligence activities. Promotes the secure and efficient execution of intelligence and counterintelligence activities at DOE and the National Nuclear Security Administration (NNSA), to include at Headquarters and throughout the national laboratory/plant/site complex and, where applicable, the Intelligence Community (IC).

2. CANCELS/SUPERSEDES. DOE O 5670.1A, *MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE*, dated 01-15-92.

3. APPLICABILITY.

   a. Departmental Applicability.

      (1) With the exception of the equivalencies/exemptions listed in paragraph 3.c., this Order applies to all Departmental elements.

      (2) The Administrator of the NNSA will assure that NNSA employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

   b. DOE Contractors.

      (1) The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Order that apply to laboratory/plant/site management contractors whose contracts include the CRD. The CRD must be included in all laboratory/plant/site management contracts.

      (2) Application of this Order to anyone other than laboratory/plant/site management contractors will be communicated separately.

      (3) Secretarial officers are responsible for communicating with Contracting Officers (COs) which laboratory/plant/site management contracts are affected by this Order. The CO is responsible for incorporating the CRD into the laws, regulations, and DOE directives clause of each affected laboratory/plant/site management contract.

(4) The laboratory/plant/site management contractor is responsible for compliance with the requirements of the CRD.

(5) Affected laboratory/plant/site management contractors are responsible for notifying subcontractors of the requirements of the CRD.

c. Equivalencies/Exemptions for DOE O 475.3.

(1) Equivalencies and exemptions to this Order are processed in accordance with DOE O 251.1, *Departmental Directives Program*, current version.

(2) In accordance with the responsibilities and authorities assigned by Executive Order (EO) 12344, codified at 50 USC 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 Order for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS.

a. It is Departmental policy that all DOE intelligence and counterintelligence activities must conform to the applicable provisions of the National Security Act of 1947, as amended; EO 12333, *United States Intelligence Activities*, as amended, and such Executive Orders as may supersede it; Department of Energy Procedures for Intelligence Activities; and all other applicable laws, Executive Orders, regulations, and directives (see section 7, References). In accordance with EO 12333 section 1.7(i)(1-2), the Office of Intelligence and Counterintelligence (IN) duties and responsibilities include:

(1) Collecting (overtly and through publicly available sources), analyzing, producing, and disseminating intelligence and counterintelligence information to support national and Departmental missions; and

(2) Conducting and participating in analytic or information exchanges with foreign partners and international organizations in accordance with EO 12333 sections 1.3(b)(4) and 1.7(a)(6).

b. The Head of the Departmental Element (HDE), or designee, must notify the CO and other appropriate subject matter experts in the organization that this Order applies to an existing contract or to a solicitation for a future contract. For existing contracts, the HDE must designate appropriate representatives to work with the CO to develop an appropriately tailored set of standards, practices, and controls.

(1) For existing management and operations (M&O) contracts, after being notified by the HDE or designee, the CO must provide the contractor with the opportunity to assess the effect of incorporating the CRD on contract

cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. All associated activities will be accomplished in a timely manner and, if applicable, in accordance with the timelines established in Department of Energy Acquisition Regulation (DEAR) 970.5204-2. The CO will incorporate the CRD without alteration.

(2) For existing non-M&O contracts, after being notified by the HDE or designee, the CO must provide the contractor the opportunity to assess the effect of incorporating the CRD on contract cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. Non-M&O contracts do not give the CO the unilateral right to modify them, except within the limitations established in the Federal Acquisition Regulation (FAR). Therefore, the CO must attempt to incorporate the CRD bilaterally. If attempts to negotiate the requirement into the contract bilaterally are not successful, the CO must consult with the Head of Contracting Activity (HCA), Headquarters program office, and General Counsel. The CO must incorporate the CRD without alteration unless the CRD or Order permits alteration and the appropriate process is followed.

5. RESPONSIBILITIES.

a. Heads of Elements of the Intelligence Community. The Secretary of Energy is the Head of DOE's Intelligence Community Element, as described in EO 12333.

b. Director, Office of Intelligence and Counterintelligence, is the designated Senior Intelligence Officer (SIO) for the Department and the Secretary's executive agent for implementing and monitoring the provisions of EO 12333 (except for those authorities and responsibilities of the Secretary, the Inspector General, and the General Counsel, which cannot be delegated), and in accordance with all relevant orders, laws, regulations, and IC Policy:

(1) Leads and manages the Department's intelligence, counterintelligence, and cyber intelligence missions and support programs.

(a) Is responsible for all intelligence, counterintelligence, and intelligence-related work performed at any DOE Federal or contractor facility, including directing the execution of the intelligence cycle on topics responsive to DOE, the IC, and the President's national security mission and priorities.

(b) Conducts and coordinates all counterintelligence policy and investigative matters with the FBI and any other applicable law-enforcement agencies, providing cooperation and assistance to those agencies when required.

(c) Oversees and coordinates the intelligence and intelligence-related reimbursable work under the Strategic Intelligence Partnership Program (SIPP) within the Department, and with its contractors.

(d) Concurs, in coordination with laboratory, plant, and site executives, the selection, appointment, and retention of Senior Intelligence Executives (SIEs), Field Intelligence Element (FIE) Directors, and Senior Counterintelligence Officers (SCIOs), who report functionally to the IN Director as designated in other DOE Orders and Procedures for Intelligence Activities, in addition to the employment relationship with their M&O employer.

(e) Enables and partners with the Departmental Elements in the use and application of intelligence information, the use of intelligence information systems, and access to any Departmental Sensitive Compartmented Information (SCI)-cleared facilities as covered by EO 12333, and as elaborated in the Secretary of Energy and Attorney General Procedures for Intelligence Activities (2017).

(2) Represents DOE's intelligence programs, products, investigations, and requirements, as applicable, to the IC, members of the Executive Branch, Congress, and foreign partners.

(a) Serves as the key interlocutor for the Department to the IC, for which IN is the only DOE element designated to produce finished intelligence products representing the Department. This also includes deconflicting, coordinating, and integrating all intelligence and counterintelligence activities with the appropriate IC elements, supporting the President's Intelligence Advisory Board and Intelligence Oversight Board, the National Intelligence Board, and the National Intelligence Council.

(b) Provides the primary channel for DOE and its contractors to request intelligence and counterintelligence support from the IC, and conversely, provide expertise, research and development, and capabilities from the Department and laboratories/plants/sites to the IC.

(c) Develops and provides all programmatic and budgetary information necessary to support the National Intelligence Program to the Director of National Intelligence (DNI), the Office of Management and Budget, and Congress.

(d) Responds to Congressional inquiries or briefing requests and disseminates finished intelligence products that are discoverable for applicable Congressional oversight committees.

(e) Serves as the primary interlocutor for the Department to foster foreign intelligence partnerships and disseminates IN information or intelligence to foreign governments and international organizations through approved intelligence or counterintelligence arrangements or agreements.

(f) Serves as the primary conduit for the Office of Office of Environment, Health, Safety and Security (EHSS) to transmit requests for updates to the Nuclear Security Threat Capabilities Assessment jointly authored by IN and the Department of Defense (DOD). Provides the DOE Office of Security and Threat Management with intelligence on new and emerging threats and updates on adversary capabilities pertinent to the security of DOE and NNSA assets in relation to DOE O 470.3, *Design Basis Threat (DBT)*.

(3) Manages DOE's intelligence and intelligence-related work, SCI, facilities, and systems, and all classified information under the purview of EO 13526 or intelligence-related work under the Atomic Energy Act of 1954, as amended, therein.

(a) Exercises original classification authority to classify information as Top Secret, Secret, or Confidential (EO 13526 section 1.3). This authority may not be redelegated.

(b) Manages the Department's SCI programs, oversees the dissemination and protection of all classified intelligence information within the Department, and develops or approves all policies, plans, procedures, and training within the Department for the protection of intelligence and intelligence sources and methods from unauthorized disclosure. This includes implementing policies and directives to adjudicate, grant, deny, and revoke access to intelligence information, including SCI.

(c) Serves as the Officially Designated Federal Security Authority (ODFSA) and Designated Accrediting Official for all DOE SCIFs, including: approving requests for construction, modification, or formally accrediting SCIFs; responsibility for SCIF security programs; and the review and adjudication of all incidents of security concern involving intelligence or intelligence-related information, including cyber incidents and counterintelligence.

(d) Serves as the Principal Authorizing Official for all DOE information systems subject to IC Directive 503, *IC Information Technology Systems Security Risk Management*, used to process, store, and transmit classified national security related intelligence information.

(e) Consults with the Director of National Intelligence concerning IC policy directives with respect to the protection of National Security Information and consults with DOE on the protection of Restricted Data and Formerly Restricted Data.

(f) Serves as the primary point of contact for IC requirements and questions regarding the use and protection of Restricted Data and Formerly Restricted Data in intelligence products, in coordination with EHSS and NNSA.

(g) Establishes policy and procedures for managing contacts between DOE and its contractor personnel with foreign governments where the purpose of the contacts involves the exchange of intelligence information or cooperation with foreign intelligence organizations.

(h) Serves as the risk acceptance authority for DOE accredited SCIFs and intelligence and intelligence-related work (including SIPP) executed within the DOE and NNSA headquarters and laboratories/plants/sites, including identifying risk and developing mitigation strategies.

(i) Supports Heads of Field Elements in mitigating or accepting shared risk for such work conducted in Hazard Category 2 and 3 nuclear facilities that operate under a Safety Basis.

(j) Advises Heads of Field Elements on potential risks identified through the vetting process for the Unclassified Foreign National Access (FNA) Program and works with them and laboratory/plant/site leadership to escalate cases lacking consensus to the HDE with cognizance for further evaluation, in accordance with DOE Order 142.3, current version.

(k) Serves as the Designated Senior Official of the Department's Insider Threat Program and is responsible for the implementation of the program.

(l) Coordinates with the Senior Agency Official for Privacy or the Chief Privacy Officer on the DOE Intelligence Element privacy program and guidance.

(m) Appoints a Civil Liberties and Privacy Officer to implement requirements of Federal law, executive order, regulation, policy, and DOE O 206.1, current version, for national security matters under the purview of the DOE Intelligence Element.

(n) Reports to the President's Intelligence Oversight Board (and concurrently to the Office of the Director of National Intelligence)

any intelligence activities that DOE has reason to believe may be unlawful or contrary to Executive Order or presidential directive.

(o) Cooperates with any Inspector General (IG) or Government Accountability Office (GAO) inquiries or investigations, while applying a need-to-know standard, as appropriate.

(p) Maintains the DOE Sensitive and other Designated Country List, which identifies a country to which a particular consideration is given for policy reasons, or reasons of national security, nuclear nonproliferation, regional instability, threat to national economic security, or terrorism support. Coordinates with NNSA and the Office of Science on the maintenance of the sensitive country list related to nonproliferation and technology transfer.

c. General Counsel provides legal guidance to Departmental organizations participating in intelligence activities and exercises those responsibilities assigned by EOs 12333 and 12334, respectively.

d. Inspector General reports, to the extent permitted by law, to the President's Intelligence Oversight Board intelligence activities that he/she has reason to believe may be unlawful or contrary to EO 12334 or Presidential directive.

e. Heads of Departmental Elements (or Designees).

(1) Ensure that all intelligence-related efforts are coordinated with IN. Coordination with IN is necessary for the following engagements by DOE Program Offices and other Departmental elements:

(a) Engagement with senior leadership of an IC element (Dash 1 and 2 level) shall be coordinated prior to the planned event;

(b) Engagement with foreign intelligence services shall be coordinated with the SIO at least three weeks prior to any planned interaction to allow time for any coordination that may be required with the broader IC;

(c) Memoranda of Agreement or Understanding with any IC element, including proposed Departmental assignees to IC elements, shall be shared with IN, preferably early in the drafting process; and

(d) Program Office sponsorship/funding of intelligence support activities with non-IC funding, including Laboratory, Plant, or Site Directed Research Development (LDRD, PDRD, SDRD) projects involving intelligence-related work at a DOE/NNSA field site shall be coordinated with IN.

(2) Work collaboratively with IN when a consensus is not reached by the SCIOs; Heads of Field Elements; and laboratory/plant/site leadership on the risks posed by an FNA request.

(3) Coordinate with IN to identify, mitigate, or accept shared risk related to the protection and use of intelligence or intelligence-related work executed by subordinate personnel.

(4) Identify and provide expertise and capabilities to IN and the IC, as applicable.

f. FIE Directors and SCIOs.

(1) Work closely with Heads of Field Elements and laboratory/plant/site leadership to ensure that appropriate processes and procedures are in place to perform all work safely, securely, and in accordance with legal and contract requirements. This includes intelligence and intelligence-related work, and more generally, ensuring that appropriate management information systems are in place. All intelligence and intelligence-related work, including SIPP, must be conducted in accordance with the contract, legal requirements, and associated statements of work. For-cause safety incidents or accident investigations can be directed by the Heads of Field Elements in close consultation with the appropriate Program Secretarial Officer and the IN Director.

(2) Provide timely access for Site or Field Office personnel to SCIFs to review documentation relevant to critical or high-risk oversight requirements, provided sensitive materials are covered or sensitive activities are otherwise protected.

(a) There is no presumption of access to SCI. Access to any intelligence or intelligence-related information, activities, SCIFs, or to SCI-level computing resources on behalf of Heads of Field Elements or their employees will be on a need-to-know basis, based on mission, critical or high-risk contract oversight requirements, and/or exigent circumstances.

g. Heads of Field Elements protect DOE's intelligence and intelligence-related work, Sensitive Compartmented Information, facilities, and systems, and all classified information under the purview of EO 13526 or the Atomic Energy Act of 1954, as amended, therein.

(1) Responsible for security, environmental, safety, and health oversight of activities at their respective sites, including those associated with the execution of intelligence and intelligence-related work and contract oversight. Site operations are conducted under approved safety, security, and other operational plans, such as Nuclear Safety Bases, Facility Safety and Security Plans, and Explosive Safety Plans.

(2) Responsible for physical security outside of IN SCIFs, with IN being the responsible Cognizant Security Authority for security programs within the SCIFs.

(a) The review and adjudication of all incidents of security concern involving intelligence or intelligence-related information, including cyber incidents and counterintelligence activities, is primarily the responsibility of IN, and will be closely coordinated with the appropriate field/site office personnel and/or senior Program Office and DOE staff office officials.

(b) IN will document security incidents and provide appropriate input to the Safeguards and Security Information Management System database, to include subsequent resolution actions.

(c) When applicable, include security incidents of concern for extent-of-condition reviews or a deeper examination for broader applicability with advanced coordination with National Laboratories/Plants/Sites.

(3) In situations where there is lack of consensus between the SCIO and the Head of the Field Element on the risks posed by an FNA request or the proposed mitigations relating to this request, the laboratory/plant/site will escalate the decision through the Heads of Field Elements to the Head of the Departmental Element with cognizance for final decision. Once at this level, the Laboratory Director; SCIO; Head of Field Element; IN Director; and IN Deputy Counterintelligence Director will convene to determine if the risk is acceptable and take all appropriate actions to mitigate the risk if the FNA request is approved.

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

7. REFERENCES.

a. *National Security Act of 1947*, as amended, Public Law (P.L.) 235 (61 STAT. 496)

b. *Atomic Energy Act of 1954*, as amended, P.L. 118-67

c. *Intelligence Authorization Act of 1995*

d. *National Defense Authorization Act (NDAA) for Fiscal Year 2020* (P.L. 116-92)

e. *John Warner NDAA Act for Fiscal Year 2007* (P.L. 109-364)

f. *NDAA for Fiscal Year 2000* (P.L. 106-65)

g. *Counterintelligence Enhancement Act of 2002* (P.L. 107-306, 50 U.S.C. Chapter 44)

h. 42 U.S.C. Sections 2011 to 2296, *Atomic Energy Act of 1954*, as amended

i. 42 U.S.C. Sections 7101 to 7352, *Department of Energy Organization Act*, as amended

j. 10 CFR Part 1045, *Nuclear Classification and Declassification*

k. 32 CFR Chapter XX, *Information Security Oversight Office*, National Archives and Records Administration

l. Exec. Order No. 12333, as amended, *United States Intelligence Community Activities*, dated 12-4-1981

m. Exec. Order No. 12334, *President's Intelligence Oversight Board*, dated 12-4-1981

n. Exec. Order No. 12968, as amended, *Access to Classified Information*, dated 8-2-1995

o. Exec. Order No. 13462, as amended by Exec. Order No. 13516 (2009), *President's Intelligence Advisory Board and Intelligence Oversight Board*, dated 02-29-2008

p. Exec. Order No. 13526, *Classified National Security Information*, dated 12-29-2009 (32 CFR Parts 2001 and 2003)

q. Exec. Order No. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, dated 10-7-2011

r. *Attorney General Approved Department of Energy Procedures for Intelligence Activities*, current version

s. Presidential Decision Directive/NSC-61, *U.S. Department of Energy Counterintelligence Program*, dated 02-11-1998

t. Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, dated 11-12-2012

u. White House Memorandum, *Early Detection of Espionage and other Intelligence Activities through the Identification and Referral of Anomalies*, dated 08-23-1996

v. SEN-6D-91, *Departmental Organizational and Management Arrangements*, dated 5-16-91

w. Delegation Order No. 00-020.00A to the Director of Intelligence and Counterintelligence, dated 3-19-2013

x. S-2 Memo *Approval of Transfer of Insider Threat Program from the Office of Environment, Health, Safety and Security to the Office of Intelligence and Counterintelligence and Appointment of the Designated Senior Official*, dated 9-2-2025

y. DOE O 142.3, *Unclassified Foreign National Access Program*, current version

z. DOE O 243.1, *Records Management Program*, current version

aa. DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*

bb. DOE O 452.8, *Control of Nuclear Weapon Data*, current version

cc. DOE O 457.1A, *Nuclear Counterterrorism*, current version

dd. DOE O 470.5, *Insider Threat Program*, current version

ee. DOE O 475.2, *Identifying Classified Information*, current version

ff. DOE O 481.1, *Strategic Partnership Projects*, current version

gg. DOE O 486.1, *DOE Foreign Government Talent Recruitment Programs*, current version

hh. DOE O 550.1, *Official Foreign Travel*, current version

ii. DOE O 5639.8, *Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities*, current version

jj. DOE P 226.1, *Department of Energy Oversight Policy*, current version

kk. DOE P 485.1, *Foreign Engagements with DOE National Laboratories*, current version

ll. Director of National Intelligence, Intelligence Community Directive (ICD) 112, *Congressional Notification*, dated 6-29-2017

mm. ICD 113, *Functional Managers*, current version

nn. ICD 116, *Intelligence Planning, Programming, Budgeting, and Evaluation System*, current version

oo. ICD 120, *IC Whistleblower Protection*, current version

pp. ICD 121, *Managing the Intelligence Community Information Environment*, current version

qq. ICD 203, *Analytic Standards*, current version

rr. ICD 205, *Analytic Outreach*, current version

ss. ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, current version

tt. ICD 207, *National Intelligence Council*, current version

uu. ICD 304, *Human Intelligence*, current version

vv. ICD 311, *Coordination of Clandestine Human and Human-enabled FI and CI inside the U.S.*, current version

ww. ICD 402, *DNI Representatives*, current version

xx. ICD 403, *Foreign Disclosure and Release of Classified National Intelligence*, current version

yy. ICD 404, *Executive Branch Intelligence Customers*, current version

zz. ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, current version

aaa. ICD 502, *Integrated Defense of the Intelligence Community Information Environment*, current version

bbb. ICD 503, *IC Information Technology Systems Security Risk Management*, current version

ccc. ICD 613, *Reciprocity for Mandatory Training*, current version

ddd. ICD 660, *IC Civilian Joint Duty Program*, current version

eee. ICD 700, *Protection of National Intelligence*, current version

fff. ICD 701, *Unauthorized Disclosures of Classified National Security Information*, current version

ggg. ICD 703, *Protection of Classified National Intelligence, Including SCI*, current version

hhh. ICD 704, *Personnel Security*, current version

iii. ICD 705, *Sensitive Compartmented Information Facilities*, current version

jjj. ICD 706, *Security Standards for Protecting Domestic IC Facilities*, current version

kkk. ICD 709, *Reciprocity for IC Employee Mobility*, current version

lll. ICD 710, *Classification and Control Markings System*, current version

mmm. ICD 712, *Requirements for Certain Employment Activities by Former Intelligence Community Employees*, current version

nnn. ICD 731, *Supply Chain Risk Management*, current version

ooo. ICD 732, *Damage Assessments*, current version

ppp. ICD 750, *Counterintelligence Programs*, current version

qqq. ICD 801, *Acquisition*, current version

rrr. ICD 900, *Integrated Mission Management*, current version

sss. ICD 906, *Controlled Access Programs*, current version

ttt. *IC Markings System*, *Register and Manual*, current version

8. DEFINITIONS.

Definitions found in current directives are listed on the Directives website: https://www.directives.doe.gov/definitions#c2=all&b_start=0

a. Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

b. Cyber Intelligence. The collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructures and data; and network characterization, or insight into the components, structures, use and vulnerabilities of foreign information systems.

c. DOE Intelligence Components.

(1) The Secretary of Energy, when acting in an intelligence capacity.

(2) IN and subordinate offices.

(a) The IN Director designates subordinate offices that include, but are not limited to, IN headquarters directorates, Field Intelligence Elements, and counterintelligence field offices.

d. DOE Intelligence Enterprise. IN Headquarters directorates, the Field Intelligence Elements, and the Counterintelligence Field Offices.

e. Foreign Intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

f. Foreign National. Anyone who is not a U.S. citizen by birth or naturalization.

g. Heads of Field Elements. Officials who direct activities of DOE/NNSA field or site offices and field organizations reporting directly to Headquarters.

h. Heads of Departmental Elements (HDE). For the purposes of this Order, HDEs include the Assistant Secretaries and Office Directors reporting to the Secretary either directly or through the Deputy Secretary or Under Secretaries. The NNSA Administrator is the only NNSA HDE. For the purposes of this Order, Power Marketing Administrators are Heads of their Departmental Elements.

i. Intelligence cycle. Consists of 1) Planning and Direction, 2) Collection, 3) Processing, 4) Analysis and Production, 5) Dissemination, 6) Evaluation and Feedback (occurs throughout the entire cycle).

j. Intelligence Information. National Security Information (NSI) relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons that would impact United States national security or foreign relations.

CONTACT. Office of Intelligence and Counterintelligence 202-586-2610.

BY ORDER OF THE SECRETARY OF ENERGY:

JAMES P. DANLY
Deputy Secretary

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 475.3, *MANAGEMENT OF THE DEPARTMENT OF ENERGY INTELLIGENCE ENTERPRISE*

This Contractor Requirements Document (CRD) establishes requirements for Department of Energy (DOE) contractors in furtherance of the management of the DOE Intelligence Enterprise as defined in this Order. Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. In accordance with Department of Energy Acquisition Regulation (DEAR) 970.5204-2, Laws, Regulations, and DOE Directives (including DEAR 952.204-78 Directives), the contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

1. REQUIREMENTS.

   a. Conform to provisions of the National Security Act of 1947, as Amended; EO 12333, as Amended, *United States Intelligence Activities*, dated 12-4-1981 and such Executive Orders as may supersede it; Department of Energy Procedures for Intelligence Activities; and all other applicable laws, Executive Orders, regulations, and directives.

   b. Work with the Contracting Officer (CO) and designated representatives to develop an appropriately tailored set of standards, practices, and controls.

   c. Assess the effect of incorporating the CRD to existing management and operations (M&O) contracts on cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. All associated activities will be accomplished in a timely manner and, if applicable, in accordance with the timelines established in DEAR 970.5204-2. The Contracting Officer will incorporate the CRD without alteration.

   d. Assess the effect of incorporating the CRD on existing non-M&O contracts cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. Non-M&O contracts do not give the CO the unilateral right to modify them, except within the limitations established in the Federal Acquisition Regulation (FAR). Therefore, the CO shall attempt to incorporate the CRD bilaterally. If attempts to negotiate the requirement into the contract bilaterally are not successful, the CO shall consult with the Head of Contracting Activity (HCA), Headquarters program office, and General Counsel. The CO shall incorporate the CRD without alteration unless the CRD or Order permits alteration and the appropriate process is followed.

   e. Provide and cooperate with any Inspector General (IG) or Government Accountability Office (GAO) inquiries or investigations, while continuing to

apply need-to-know as appropriate.

f. Provide robust support to and participation in the Department's Insider Threat Program in accordance with DOE Order 470.5, and its successors.

g. Contractors assigned to support the IN mission shall, at the direction of IN, perform:

(1) Intelligence, counterintelligence, and intelligence-related work at assigned DOE Federal or contractor facilities.

(2) Intelligence cycle collection and analysis on topics responsive to DOE, the IC, and the President's national security mission and priorities.

(3) Counterintelligence policy and investigative matters in accordance with IN Counterintelligence Directorate guidelines.

(4) Intelligence and intelligence-related reimbursable work under the Strategic Intelligence Partnership Program (SIPP).

2. RESPONSIBILITIES.

a. Laboratory/Plant/Site Leadership.

(1) Submit for concurrence from the Director, Office of Intelligence and Counterintelligence (IN) the selection, appointment, and retention of Senior Intelligence Executives (SIEs), Field Intelligence Element (FIE) Directors, and Senior Counterintelligence Officers (SCIOs), who functionally report to the IN Director as designated in other DOE Orders and Procedures for Intelligence Activities, in addition to the employment relationship with their M&O employer.

(2) Escalate decisions to the program office at the Under Secretary (US) level in situations where there is lack of consensus between the SCIO and laboratory/plant/site and the Heads of the Field Elements on the risks posed by national laboratory/plant/site foreign external engagements or involvements.

(a) Once at the US level (including the relevant program office assistant secretary), the Laboratory/Plant/Site Director; Head of the Field Element; SCIO; IN Director; and IN Deputy Counterintelligence Director; will convene to determine final risk acceptance or denial and approve actions to mitigate the risk if the foreign entity or involvement is approved.

b. FIE Directors and SCIOs.

(1) Work closely with Heads of Field Elements and laboratory/plant/site leadership to ensure that appropriate processes and procedures are in place to perform all work safely, securely, and in accordance with legal and contract requirements. This includes intelligence and intelligence-related work, and more generally, ensuring that appropriate management information systems are in place. All intelligence and intelligence-related work, including SIPP, must be conducted in accordance with the contract, legal requirements, and associated statements of work. For-cause safety incidents or accident investigations can be directed by the Heads of Field Elements in close consultation with the appropriate Program Secretarial Officer and the IN Director.

(2) Provide timely access for Site or Field Office personnel to SCIFs to review documentation relevant to critical or high-risk oversight requirements, provided sensitive materials are covered or sensitive activities are otherwise protected.

(a) There is no presumption of access to SCI. Access to any intelligence or intelligence-related information, activities, SCIFs, or to SCI-level computing resources on behalf of Heads of Field Elements or their employees will be on a need-to-know basis, based on mission, critical or high-risk contract oversight requirements, and/or exigent circumstances.

c. Contractors assigned to DOE and NNSA.

(1) If required for the performance of their duties, request intelligence and counterintelligence support from the IC or, conversely, provide Departmental expertise and capabilities to the IC through IN.

(2) Identify and provide expertise and capabilities to IN and the IC, as applicable.

(3) Counterintelligence Headquarters and Counterintelligence Field Offices are required to conduct reviews for many national laboratory/plant/site foreign engagements or interactions (including entity foreign ownership or foreign involvement). Reviews include the Unclassified Foreign National Access Program, Strategic Partnership Programs and Cooperative Research and Development Agreements, and others.