U.S. Department of Energy
Washington, DC

ORDER

DOE O 470.1A

Approved: 12-18-2024

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM MANAGEMENT OPERATIONS

1. PURPOSE. Establish the U.S. Department of Energy (DOE) Safeguards and Security (S&S) Program Management Operations requirements as promulgated in laws, regulations, Executive Orders (EO), and national standards established to prevent adverse impacts on national security and mitigate unacceptable risks. This Order addresses facility clearance (FCL) (also known as entity eligibility determinations) requirements; foreign ownership, control, or influence (FOCI) determinations; classified mail channels; classified visits within the Department, including foreign classified visits; and incidents of security concern (IOSC).

2. CANCELS/SUPERSEDES.

   a. This Order hereby cancels the portions of DOE Order (O) 470.4B Chg 3 (LtdChg), *Safeguards and Security Program*, that relate to S&S Program Management Operations. DOE O 470.4C, *Safeguards and Security Planning*, cancels the S&S Planning portions of DOE O 470.4B Chg 3.

   b. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs [Attachment 1]) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. Except for the equivalencies/exemptions in paragraph 3.c., this Order applies to all cleared Departmental elements. The Administrator of the National Nuclear Security Administration (NNSA) must ensure that NNSA employees and contractors 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 Public Law (P.L.) 106-65 to establish Administration specific policies, unless disapproved by the Secretary.

2. DOE Contractors. Attachment 1 sets forth the requirements of this Order that will apply to contracts that include the CRD or its requirements.

The CRD and its requirements must be included in all contracts (primary and subcontracts) that involve security activities[1], require access to national security assets, and/or contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

a. Contractors are responsible for incorporating the CRD and its requirements into their affected subcontracts.

3. Equivalencies/Exemptions for DOE O 470.1. Equivalencies and exemptions from the requirements of this Order are processed in accordance with the current DOE O 251.1, *Departmental Directives Program*, current version.

a. Requests must be based on an informed risk management decision.

b. When applicable, the requesting organization must document and accept the security risk in accordance with applicable authorities.

c. The requesting organization must consult with their relevant General Counsel (GC) and the Office of Environment, Health, Safety, and Security (EHSS), Office of Security (EHSS-50) before submitting the request for approval. The Office of Security must respond to consultation request within 45 days from receipt of the request.

d. Approved equivalencies and exemptions must be entered into the Safeguards and Security Information Management System (SSIMS) database and incorporated into the approved security plan(s) to be effective for operations.

e. DOE S&S program requirements may also be located in, or based upon, regulations issued by Federal agencies, and codified in the Code of Federal Regulations (CFRs), or other authorities, such as Executive Orders (EO) 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, DOE GC, or NNSA GC, must be consulted to determine whether the Departmental Element's deviation from the source can be legally pursued.

f. Existing equivalencies and exemptions must be reviewed to determine relevancy and applicability to the requirements set forth in this Order.

(1) Existing equivalencies and exemptions must be reviewed to determine applicability under DOE O 470.1, current version. If applicable, the site must document the review was completed and the equivalency or exemption remains valid.

(2) Equivalency. In accordance with the responsibilities and authorities

[1] "Safeguards and Security Activity" is also known as security activity. The terms "safeguards and security activity" and "security activities" are used interchangeably throughout this Order. See Attachment 7 for Definitions.

assigned by 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 Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS.

a. General.

(1) Departmental Elements must ensure S&S programs implement the requirements found in the Attachments to this Order and all supportive contracts that include this CRD, or its requirements as specified by the contracting officer.

(2) Whenever a legal, regulatory, or other external standard, or a DOE directive referenced within this Order is amended or superseded, the current version is applicable under this Order.

(3) S&S programs must implement and maintain S&S operations management roles, responsibilities, and requirements contained in this Directive.

(4) Programs associated with each topical area within this Order must be implemented in accordance with the requirements for that topic.

(5) S&S program management operations and implementation procedures must be documented in the approved security plan in accordance with DOE O 470.4, *Safeguards and Security Planning,* current version.

(6) Incidents of security concern must be addressed in accordance with the requirements found in Attachment 6 and reported in accordance with applicable laws and regulations.

(7) S&S program management operations must be thoroughly integrated with other Departmental programs to coordinate related security activities addressed in this Order, including Safety, Emergency Management, Personnel Security, Insider Threat, Contracts and Procurements, Counterintelligence, FCL and FOCI program, GC (as appropriate), and Federal oversight organizations.[2]

b. Delegation of S&S Authorities.

(1) Delegation of authority to Officially Designated Federal Security

[2] See paragraph 4., "Responsibilities," "Office of General Counsel (GC)".

Authority (ODFSA) or Officially Designated Security Authority (ODSA) is implemented according to direction from the accountable Program Secretarial Officer (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Officer) who also provides direction for further delegation beyond the primary delegation.

(2) Each delegation must be formally documented. It may be included in other security plans or documentation approved by or according to direction from the office which is delegating authority.

(3) Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation.

c. Implementation.

(1) After being notified by the Head of the Departmental Element or designee, the Contracting Officer (CO) must incorporate the Contractor Requirements Document (CRD) in Attachment 1 in existing applicable contracts per the process described in DOE O 251.1, Departmental Directives Program, current version.

(2) Compliance with the requirements within this Order, including the Attachments, must be complete within one (1) year of the issuance date.

(3) If compliance cannot be accomplished within one (1) year, an implementation schedule must be submitted to the appropriate Cognizant Security Office (CSO), prior to this deadline.

(4) The documentation must include timelines and resources needed to fully implement this Order as well as a description of the vulnerabilities and impacts created by the delay.

(5) Implementation plans must be referenced in the security plan.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Ensures that effective S&S program management operations are established, executed, and maintained within DOE under the authorities granted by relevant Executive Orders; the U.S. Department of Energy Organization Act, as amended (42 U.S.C. Sections 7101 to 7352); and Atomic Energy Act, as amended (42 U.S.C. Sections 2011 to 2286), and in accordance with P.L. 106-65, the National Nuclear Security Administration Act.

(2) Designates senior Departmental officials to direct S&S program operations management procedures.

(3) Delegates, in writing, all responsibilities and authorities as necessary for the administration of the S&S program operations.

(4) Exercises sole authority to approve the imposition of requirements for programs and activities that are more stringent and/or comprehensive than those imposed by the Nuclear Regulatory Commission (NRC).

b. Deputy Secretary.

(1) Exercises responsibility, as Chief Operating Officer of the Department, for S&S policy development and operations.

(2) Approves all S&S Directives.

(3) In accordance with 50 U.S.C. Section 2656, ensures that the Committees on Armed Services of the U.S. House of Representatives and the U.S. Senate are notified of each significant nuclear defense intelligence loss.

c. Under Secretary for Nuclear Security/Administrator for the National Nuclear Security Administration.

(1) Responsible for the management and implementation of S&S programs administered by NNSA and its subordinate offices, including provision of the appropriate level of authorities and resources to effectively manage and execute S&S responsibilities.

(2) Responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA.

(3) Through the Deputy Administrator for Defense Programs:

(a) Ensures that all classified visits in connection with the military application of atomic energy under 42 U.S.C. Section 2164 and 42 U.S.C. Section 2121 are conducted in accordance with National and Departmental policies and governing international agreements or treaties.

(b) Approves requests for access to weapons programs and classified information pertaining to Nuclear Weapons Data (NWD).

(4) Through the Deputy Administrator for Defense Nuclear Nonproliferation,

Ensures that all classified visits in connection with nonproliferation, international security, or International Atomic Energy Agency requirements are conducted in accordance with National and Departmental policies and governing international agreements or treaties.

(5) Through the Deputy Administrator for Naval Reactors:

(a) Ensures that all classified visits in connection with naval nuclear propulsion are conducted in accordance with National and Departmental policies and governing international agreements or treaties.

(b) Approves requests for classified visits and access to naval nuclear propulsion facilities.

(6) Through the Associate Administrator and Chief for Defense Nuclear Security:

(a) Responsible for the development and implementation of security programs for the Administration, including the protection, control and accounting of materials, and for the physical security for all facilities of the NNSA.

(b) Acts as Senior NNSA official responsible for the direction and administration of the NNSA implementation and compliance with the National Industrial Security Program.

(c) Acts as the Senior NNSA official responsible for classified visits except for those assigned to the Deputy Administrator for Defense Programs; delegates in writing to a senior Federal official at each NNSA site the authority to take a risk-based approach to oversee the classified visits program for granting access to RD.

(d) Implements DOE's North Atlantic Treaty Organization (NATO) program for DOE and NNSA including access authorizations, policy, operations of the DOE Sub-Registry, and the conduct of DOE domestic inspections.

d. Office of Environment, Health, Safety and Security (EHSS).

(1) Develops, coordinates and promulgates the Department's S&S policies and procedures to ensure a comprehensive S&S Program consistent with the Department's statutory authorities, mission, and national-level policies.

(2) Oversees DOE Headquarters CSOs and delegates this authority in writing as appropriate.

(3) Oversees implementation of DOE Headquarters S&S program operations, including the development of S&S program management operations implementation procedures and guidance.

(4) Serves as the Approval Authority of Headquarters equivalencies and exemptions.

(5) Provides S&S program management operations implementation guidance and assistance for DOE offices located in Headquarters facilities.

(6) Provides S&S program management operations advice and assistance to Departmental organizations.

(7) Maintains national-level liaison with Federal and local law enforcement, security, and intelligence agencies to support DOE's S&S program management operations.

(8) Represents DOE in interagency efforts related to S&S activities.

(9) Acts as the Senior Agency Official responsible for direction and implementation of DOE's implementation of and compliance with the NISP.

(10) Annually report NISP-related costs and implementation metrics to the Information Security Oversight Office (ISOO).

e. Program Secretarial Officer.

(1) Ensures S&S programs are effectively and efficiently managed and implemented throughout the organization.

(2) Designates the CSO under their purview in addition to those designated per 32 CFR 117.

(3) Provides guidance and oversight to CSOs under their purview that oversee programs utilizing Departmental assets for the purposes of protecting S&S interests.

(4) Records and reports required NISP-related costs and implementation metrics to EHSS per 32 CFR 2004.

(5) Ensures that all classified visits are conducted in accordance with National and Departmental policies and governing international agreements or treaties.

f. Cognizant Security Offices.[3] CSOs are designated by the Program Secretarial Officer or, for NNSA, the Office of the Administrator through the Associate Administrator and Chief for Defense Nuclear Security.

(1) CSOs administer and oversee assigned S&S program management operations activities for their sites and facilities on behalf of the Program Secretarial Officer.

(2) CSO responsibilities for each topical area are conveyed within the

[3] As defined in Attachment 7

Attachments of this Order.

(3) Industrial Security Service Provider render facility clearances, FOCI determinations, and/or other industrial security-related services on behalf of the CSO.

g. Heads of Field Elements and Headquarters Departmental Elements.

(1) Oversee the development of S&S plans that describe S&S program management operations implementation procedures.

(2) Develop and/or allocate budgets and resources to maintain effective S&S program management operations.

(3) Provide S&S program management operations supplemental guidance and directs implementation procedures.

(4) Ensure that line management implements the applicable provisions of programs described in this Order.

(5) Communicate to contracting officers the security requirements for contracts that require the performance of security activities and/or access to security assets.

(6) Ensure that contracting officers provide DOE F 470.1, Contract Security Classification Specification (CSCS), to the CSO and/or its designee.

(7) Consult with the Office of Security prior to modifying or withholding any requirements in this Order from a contract.

(8) Ensure that contractors and subcontractors under their cognizance implement the provisions of the CRD and attachments to this Order when the CRD is incorporated in their contracts.

h. Officially Designated Federal Security Authority (ODFSA).

(1) Executes requirements and responsibilities that are formally delegated from DOE or NNSA

(2) Reviews and approves contractor security plans, establishing a Federally approved authorization for site security operations.

(3) Accepts or transmits the security risk associated with the assets under their cognizance, in accordance with DOE O 470.3, current version.

(4) Performs S&S program management operations activities as prescribed in this Order.

(5) Ensure that a senior Federal official at each site under their cognizance has been delegated in writing the authority to make, in connection with classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data (RD) will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

i. Officially Designated Security Authority (ODSA).

(1) Executes requirements and responsibilities that are formally delegated from DOE or NNSA.

(2) Performs delegated S&S program management operations activities prescribes within the Attachments of this Order.

j. Office of Enterprise Assessments.

(1) Performs assessments and reports to the Secretary on the Department's S&S programs.

(2) Implements the procedures for the assessment of civil penalties set forth in 10 CFR Part 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

(3) Develops and provides S&S program management operations training programs through the National Training Center (NTC).

(4) Through the NTC, certifies site implementation of NTC-developed courses, establishes the Training Approval Program for S&S programs, and approves site training programs.

k. Contracting Officers.

(1) Upon notification of applicability, incorporate the CRD into affected contracts via the appropriate process.

(2) Assist Government Contracting Activities (GCAs) with developing contract solicitations to incorporate the requirements of this Order.

(3) Contracting Officers must consult with the Head of Departmental or Field Element to propose any modification or withholding of any requirements in this Order from a contract.

(4) Provide written notification to the CSO in accordance with Attachment 3, "Foreign Ownership, Control, or Influence", of this Order when contractual changes impacting a company's foreign ownership, control, or influence occur.

(5) DOE Contracting Officers and the Primary contractor must ensure the CRD, applicable security requirements, and DEAR clauses are incorporated into the tiered subcontracts under their cognizance.

(6) Maintain cognizance of subcontracts with performance of security activities and/or access to security assets for contract performance.

(7) Reviews procurement requests for new contracts and ensures that the provisions of 48 CFR Section 952.204-2, Security Requirements, and the requirements of the CRD and its attachments in this Order are included in the contracts when required.

l. Office of the General Counsel (GC)[4].

(1) Provides legal advice and assistance regarding issues or changes in laws and regulations that affect S&S programs and interests.

(2) Provides legal advice on S&S program management operations requirements prescribed in this Order.

(3) Reviews and provides legal advice and assistance regarding foreign ownership, control, or influence (FOCI) mitigation strategies and National Interest Determinations (NIDs).

m. Office of Intelligence and Counterintelligence.

(1) Shares relevant information developed through intelligence/counterintelligence program activities with appropriate offices.

(2) Interfaces and interacts with S&S programs to ensure Sensitive Compartmented Information (SCI) requirements are identified, defined, and maintained, when applicable.

(3) Notifies the ODFSA, or designee, of security incidents during intelligence/counterintelligence activities. This notification will be upon discovery unless such notification would severely impede or negate intelligence activities or counterintelligence investigations, or further compromise classified/sensitive information.

(4) Ensures that all classified visits in connection with SCI are conducted in accordance with governing National and Departmental policies and international agreements or treaties.

[4] For the purposes of this Directive, the "Office of General Counsel" or "General Counsel" represents the DOE Office of the General Counsel (DOE GC), and NNSA Office of General Counsel (NA-GC), unless otherwise specifically stated.

(5) Ensures that information on relevant intelligence/counterintelligence concerns is provided to Departmental elements responsible for classified visits by foreign nationals under international agreements and treaties and to individuals responsible for hosting classified visits by foreign nationals to DOE facilities and sites.

6. INVOKED STANDARDS.[5]

a. This Order does not invoke any DOE technical standards or industry standards as required methods.

b. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order.

7. DEFINITIONS.

a. Terms commonly used in the DOE Safeguards and Security Program are defined within Attachment 7 of this Order, and in the DOE Policy Information Resource (PIR) tool located at https://pir.doe.gov/.

b. Terms specific to an Attachment are defined within that Attachment.

8. REFERENCES.

a. Attachment 8 contains the list of referenced documents within this Directive.

b. DOE Orders referenced in this Order are located on the DOE Directives webpage, https://www.directives.doe.gov/.

c. DOE Technical Standards referenced in this Order are located on the DOE Technical Standards webpage, https://www.standards.doe.gov/.

d. All other referenced materials are located on the DOE PIR tool, https://pir.doe.gov/.

9. CONTACT.

a. Questions concerning this Order should be directed to the Office of Security Policy, Office of Environment, Health, Safety and Security, email address Security.Directives@hq.doe.gov.

b. Formal policy clarification requests must be submitted to the Director, Office of Security through the respective Program Office.

c. Questions regarding implementation requirements and procedures should be directed through to the requestor’s respective line management channels.

[5] DOE O 251.1, current version, defines "invoked technical standard."

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

TABLE OF CONTENTS

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
DOE O 470.1A, SAFEGUARDS AND SECURITY PROGRAM MANAGEMENT OPERATIONS

This CRD establishes the U.S. Department of Energy (DOE) requirements for conducting management activities connected with the operation of cleared facilities within the DOE complex.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments 2 - 8 to DOE O 470.1, current version. Each Attachment provides program requirements and/or information that is applicable to contracts in which this CRD and/or DEAR Clause 952.204-2 is inserted or must be applied.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. 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.

A violation of the provisions of the CRD and/or contract security requirements to protect and safeguard national security assets may result in a civil penalty pursuant to the *Atomic Energy Act* (42 U.S.C. Section 2282b), Section 234B Subsection A. The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.*

ATTACHMENT 2
FACILITY CLEARANCES (FCL)AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. OBJECTIVE. To ensure that DOE, DOE contractor, and other (Federal) government agency (OGA) facilities and their contractors engaged in DOE activities are eligible for access to, and meet the requirements to possess and secure, classified information or matter or special nuclear material (SNM)/other accountable nuclear material (OANM); and, as applicable, to protect other assets and conduct other security activities on behalf of DOE.

2. PURPOSE. The FCL program regulates DOE approval of a Federal or contractor facility's eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter; SNM/OANM; other hazardous material presenting a potential radiological, chemical, or biological sabotage threat; and/or DOE property of significant monetary value, exclusive of facilities and land values (hereinafter referred to as security assets and activities).

3. GENERAL.

   a. This Attachment establishes the requirements that ensure DOE, DOE contractor entities, and Cognizant Security Agency (CSA) facilities and their contractor entities that are engaged in DOE security activities are eligible for access to and meet the requirements to access, possess, and secure security assets on behalf of DOE.

   b. The Department of Energy Acquisition Regulation (DEAR) Subpart 904.70, "Facility Clearance" and Subpart 952.204-73, "Facility Clearance" are incorporated into contracts for the protection security activities and assets.

   c. The 32 CFR 117, *National Industrial Security Program Operating Manual (NISPOM),* current version, serves as a national standard to establish the baseline requirements for contractor FCLs when contractors are engaged in security activities requiring the protection of national security information classified at the Confidential, Secret, or Top Secret (TS) level.

4. REQUIREMENTS. An entity (federal or contractor) must ensure that the following activities are accomplished for their FCL program and by entities under their cognizance.

   a. Establish and maintain FCL activities in accordance with the requirements contained in this Order.

   b. Provide required information to the Cognizant Security Officer (CSO) and/or the

Industrial Security Service Provider (ISSP)[6] to ascertain risk and if classified information and other security assets are adequately protected to make an FCL determination.

c. Ensure the DOE F 470.2, *Facility Data and Approval Record (FDAR)*, DOE F 470.1, *Contract Security Classification Specification (CSCS)* and other information pertaining to FCLs are accurately entered and maintained in the Safeguards and Security Information Management System (SSIMS).

d. CSOs must ensure that key management personnel (KMP) that must be cleared in connection with the FCL, possess and maintain DOE personnel security clearances (PCLs) at or higher than the FCL that is required for contract performance.

e. CSOs must ensure that entities have an active DOE FCL prior to engaging in security activities and/or accessing or possessing security assets.

f. Changes that affect a cleared entity must be reported to the CSO and any other DOE federal authorities.

g. Establish internal procedures to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the Facility Security Officer (FSO), appropriate DOE authorities (including Counterintelligence), the Federal Bureau of Investigation, or other Federal authorities as required by DOE directives, the terms of the classified contract, and U.S. law.[7]

h. Cooperate with DOE and other federal authorities during the FOCI/FCL process, official surveys and investigations concerning the protection of classified information and DOE security interests, and during access authorization investigations.

i. Maintain all records pertaining to the FCL, including original records in accordance with National Archives and Records Administration (NARA) records retention schedule.

j. Document FCL program procedures in the approved security plans.

[6] For the purposes of this Attachment, CSO and ISSP may be interchangeable to identify FCL responsibilities.

[7] The term "Classified Contract" refers to any procurement vehicle that involves security activities and/or access to security assets, that requires an FCL and personnel security clearances (PCL) also called access authorizations).

ATTACHMENT 2
SECTION 1: FCL PROGRAM

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL.

   a. DOE federal facilities:

      (1) That possess security assets require an FCL and must be registered as Possessing with a Facility Code.

      (2) Whose employees require PCLs must have a commensurate FCL with a Facility Code.

   b. Government-Owned, Contractor-Operated (GOCO) facilities with security assets and/or security activities require an FCL and must be registered as Possessing or Non- possessing with a Facility Code.

   c. Management and Operating (M&O) contractors awarded the contract for the GOCO must:

      (1) Have a separate FCL from the GOCO.

      (2) The GOCO, DOE Form 470.2, *Facility Data and Approval Record (FDAR),* will reflect the Possessing or Non-Possessing approvals for the GOCO facility.

      (3) The M&O contractor must have a separate FCL approval at the same or higher classification level/category for access only.

   d. State, local, tribal, and other similar governmental authorities do not have authority to self-certify clearances to engage in security activities. These entities must be handled in accordance with E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, and its implementing directives.

   e. Entities at any tier will require an FCL when the terms of the contract awarded include access to security assets and/or engagement in security activities and described as a "possessing" or "non-possessing" facility.

   f. An entity at any tier requiring an FCL must be sponsored by:

      (1) A Government Contracting Activity (GCA).

(2) A cleared contractor acting as the prime contractor for an uncleared subcontractor.

(3) A contractor cannot sponsor itself for an FCL.

g. Contractors whose employees require PCLs for contract performance must have an FCL commensurate with the assets to be protected.

h. A contractor or prospective contractor must meet the following eligibility requirements prior to being processed for an FCL:

(1) Be selected to perform tasks under a contract containing the DEAR security clauses found in 48 CFR Part 952; and

(2) Be organized under the laws of one of the 50 States, the District of Columbia, or Puerto Rico and must be located in the United States or a U.S. territorial area or possession;

(3) Have a reputation for integrity and lawful conduct in its business operations and relationships;

(4) Not have been barred from participating in U.S. Government contracts (this includes key management on the contract); and

(5) Not be under foreign ownership, control, or influence (FOCI) to a degree that the granting or continuation of the FCL would be inconsistent with the national interest.

ATTACHMENT 2
SECTION 2: FCL CODES

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL.

   a. Each federal or contractor entity that will access security assets or engage in security activities must be identified with a Facility Code in SSIMS.

   b. The entity's Facility Code must be recorded on the FDAR.

2. REQUIREMENTS.

   a. Facility Code. For purposes of granting and registering a FCL in SSIMS, an entity (federal or contractor) and its security activities must be registered with one facility code when the following criteria are met:

      (1) A centrally directed security program is maintained that covers all security activities (i.e., under the same name, single mailing address, single security plan applicable at all locations, and all security matters under a single management control).

      (2) The physical distance between the facilities does not inhibit day-to-day observations of the security program by the appointed Facility Security Officer (FSO).

      (3) The security activities are such that the Federal or contractor entity can maintain daily observations and oversight of its security programs and operations.

   b. Entities that cannot be registered under one Facility Code as outlined above, must be registered with a separate Facility Code.

   c. Possessing.

      (1) A possessor is any entity that will safeguard (receive, generate, reproduce, store, transmit and/or destroy) classified matter, and/or SNM at the entity's physical location as registered in SSIMS.

      (2) FDAR must be properly completed and identify the security assets that the entity is authorized to access and store.

         (a) Access – highest classification level/category of classified to be accessed to include any special accesses.

(b) Classified Storage Capability – highest classification level/category of classified approved at the entity's facility to include any special accesses.

(c) Nuclear Materials, specifically:

1 Special Nuclear Material (SNM) – attractiveness level and category of SNM requiring material controls and accountability program.

a Highest category of Material Balance Area (i.e., Category I, II, III, or IV).

b Onsite total rollup quantities (regardless of credibility) of SNM categories (i.e., Category I, II, III, or IV).

2 Other Accountable Nuclear Materials (OANM) requires accountability program.

(d) Additional Considerations:

1 If the asset is considered National Critical Infrastructure as determined by DOE line management.

2 If the assets include certain categories of biological agents.

3 If government property of a significant monetary value (e.g. $5M or as determined by Program Office and/or DOE Line Management).

4 If the entity has responsibilities related to DOE program continuity.

5 If there are national security considerations; or

6 If the entity or assets involve responsibilities for protection of the health and safety of the public and employees.

d. Non-Possessing. Any entity that will not safeguard (receive, generate, reproduce, store, transmit and/or destroy) classified matter, and/or SNM at the entity's physical location as registered in SSIMS but will require PCLs for the employees to perform work at other possessing facilities.

e. Self-Employed Individual.

(1) An individual who is self-employed/a sole proprietor not doing business as a legal entity (i.e., paid to Social Security Number) and does not require an FCL, provided the individual is the sole employee requiring a PCL and is performing as a consultant.

(2) An individual who will possess classified information or matter at their place of business must be processed for and granted an FCL.

(a) The FCL must apply to the location where the individual will receive, generate, reproduce, store, transmit, and/or destroy classified information or matter.

(b) Possessing self-employed individuals must implement the requirements set forth in this Order.

f. Prime/Subcontractor.

(1) A prime contract can be a possessing or non-possessing facility. A prime contractor must have an FCL at the same, or higher access level as its subcontractors.

(2) The subcontractor may be registered as a possessing facility while the prime contractor is registered as a non-possessor if the FCL level is the same.

g. Multiple Facility Organization (MFOs).

(3) The home office facility must have an FCL at the same, or higher access level as that of any facility (e.g., branch or division office) within the MFO.

(4) The branch/division facility may be registered as a possessing facility while the home office is registered as a non-possessor if the FCL access level is the same.

h. Parent/Subsidiary.

(1) In a corporate tier parent-subsidiary relationship, the parent and each of its subsidiaries are separate legal entities and must be processed separately for an FCL.

(2) CSOs must determine the necessity for the parent to be cleared or excluded from access.

(3) CSOs must advise the entity on what action is necessary to process the FCL.

(a) Subject to DOE approval, when a parent or its cleared subsidiaries are co-located, a formal written agreement to use common security services may be executed by all firms.

(b) The subsidiary facility may be registered as a possessing facility while the parent is registered as a non-possessor or excluded parent.

i. Excluded Parent. A corporate tier parent of a contractor organization when the parent has been formally excluded through the Foreign Ownership, Control, or Influence (FOCI) Program from participation in the activities related to a contract with DOE.

j. Joint Ventures (JVs).

(1) A JV established as a legal business entity must be granted an FCL commensurate to the security activity.

(a) Each JV partner must be granted an FCL commensurate to the security activity.

(b) As determined by the CSO, JV partners that do not impact the JV's operations, security activities, and/or assets may be excluded in accordance with the requirements set forth in this Attachment.

(c) Cleared partners that participate in security activities must ensure uncleared partners are not granted access to security assets.

(2) The JV must appoint in writing a Senior Management Official (SMO), and other KMP as determined by the CSO.

(3) The JV SMO must appoint in writing, an employee, or multiple employees as the Insider Threat Program Senior Official (ITPSO) and FSO, that must obtain and maintain a DOE PCL in connection with the FCL.[8]

k. Upgrading and Downgrading an FCL.

(1) CSO must evaluate each approved facility as security activities are added or changed to ensure the FDAR is accurate.

(2) CSO must determine if the changes require a transfer of the CSO based on the level of security assets.

l. Transferring FCL Cognizance.

(1) When a transfer of cognizance applies:

(a) CSOs and/or ISSPs must notify the receiving CSO and/or ISSP of transfer,

(b) The receiving CSOs and/or ISSPs must request to transfer the active or in process KMP PCLs within the agreed upon timeframe, and

(c) A favorable FOCI determination is rendered prior to transferring FCL cognizance.

(2) CSOs and/or ISSPs must update SSIMS to reflect the transfer of cognizance on the FDAR.

ATTACHMENT 2
SECTION 3: FCL APPROVAL REQUIREMENTS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. DOE FEDERAL FACILITIES. All eligibility requirements listed below must be satisfied prior to the issuance of an FCL.

   a. Must be registered in SSIMS with a Facility Code.

   b. A final FCL must be based on the following items:

      (1) Approved safeguards and security plan, developed in accordance with DOE O 470.4, *Safeguards and Security Planning,* current version.

      (2) Completed self-assessment per DOE O 470.4, current version.

2. CONTRACTOR FACILITIES.

   a. The DOE Acquisition Regulation (DEAR) prohibits the award of a contract requiring access to classified information or matter until a favorable FOCI determination has been rendered.

   b. The appropriate DEAR Security Clause must be applied to the contract when an existing unclassified contract is modified to require classified work. The classified work must not take place until the contract is modified and the appropriate FCL is issued.

   c. A contractor's final FCL must be based on the following items:

      (1) A favorable foreign ownership, control, or influence (FOCI) determination.

      (2) A contract or proposed contract containing the appropriate security clauses found in the DEAR.

      (3) Security plan approved by the Officially Designated Federal Security Authority, developed in accordance with DOE O 470.4, current version, and other directives, which describe protective measures appropriate to the activities being performed at the facility.

      (4) KMP, including the SMO, FSO and ITPSO, must currently possess a PCL equivalent to, or higher than, the FCL level.[8]

[8] An interim FCL can be granted pending the grant of the final DOE personnel security clearances.

(5) The SMO must appoint the FSO and ITPSO, in writing. The SMO, FSO, and ITPSO KMP roles can be held by the same person.

(6) The SMO, FSO and ITPSO must be a U.S. citizen and an employee of the contractor entity.

d. FSO and ITPSO training must be completed within 6 months of appointment to the position.

e. In addition to the above, for Possessing facilities:

(1) If possession of SNM and/or OANM is involved, the facility:

(a) Must have an established Reporting Identification Symbol code for the Nuclear Materials Management and Safeguards System (NMMSS) Reporting.

(b) Must have an appointed Nuclear Materials Representative, in accordance with, DOE O 474.2, *Nuclear Material Control and Accountability*, current version, who is responsible for reporting to NMMSS.

(2) An initial survey:

(a) Must be conducted no more than 6 months before the FCL is granted; and

(b) Must be conducted in accordance with DOE O 470.4, current version.

ATTACHMENT 2
SECTION 4: FCL RECIPROCITY

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL.

   a. When a contractor has an appropriate final FCL, DOE will not duplicate the final FCL processes performed by a CSA.[9]

      (1) When DOE cannot obtain acknowledgement from the CSA, the contractor may be subject to duplicate processing.

      (2) CSOs are not required to verify FSO training for FCLs under reciprocity.

   b. A contractor with an equal or higher FCL granted by a CSA under the NISP may be accepted by DOE for accessing, receiving, generating, reproducing, storing, transmitting, or destroying classified information or matter, or other security asset, contingent on the conditions listed below.

   c. Reciprocity between DOE and the CSA must be documented in a written letter or memorandum of agreement between the DOE cognizant security office (CSO) and the CSA that establishes the responsibilities of each party for assurance and verification of the protection afforded the DOE assets.

2. REQUIREMENTS.

   a. Accepting CSA FCLs.

      (1) Classification Level/Category and Special Conditions. The FCL granted by the CSA must be at the appropriate classification level and category and must encompass the DOE security activity.

         (a) Limited or interim FCLs granted by a CSA cannot be accepted.

         (b) DOE may not enter reciprocity with a CSA for the protection of SNM and/or OANM.If the CSA contractor is cleared under a FOCI mitigation, the CSO must obtain a copy of the FOCI mitigation

[9] The phrase "appropriate final FCL" or "appropriate FCL" represents the FCL (or EED), needed to access the classification level, caveat, and/or sensitivity level of security assets and security activities required for contract performance. This phrase is indicative that no outstanding or pending PCL, FCL, or FOCI determinations or actions remain.

plan. The mitigation plan must be submitted to EHSS or Chief for Defense Nuclear Security, as appropriate.

(c) When the company is controlled by a foreign government, the foreign government interest must be mitigated or negated in accordance with Attachment 3 of this Directive.

(d) For DOE contracts involving proscribed information (i.e., Top Secret, Restricted Data, COMSEC, SAP, and SCI), the following requirements, as appropriate, must be met before accepting an FCL granted in conjunction with a Special Security Agreement (SSA) or Security Control Agreement (SCA).

When the company is controlled by a foreign government:

1 DOE must have entered into an agreement with the foreign government involved that covers the proscribed information to be released under the contract; and

2 A waiver must be granted by the cognizant Secretary (i.e., the Secretary of Energy and/or the Secretary of Defense) in accordance with the provisions of 10 U.S.C. Section 2536, Award of certain contracts to entities controlled by a foreign government: prohibition, which prohibits contract awards involving proscribed information to foreign government-controlled companies unless such a waiver is granted.

(2) A CSA Top Secret FCL can be utilized to grant a DOE Secret/RD non-possessing or possessing interest.

KMP for possessing (safeguarding) interests must possess DOE PCLs at the appropriate level.

(3) A CSA Secret FCL can be utilized to grant a DOE Secret/RD non-possessing interest. All KMP and individuals requiring access to Secret/RD must possess DOE PCLs at the appropriate level.

(4) If the personnel security clearances are not at the appropriate level, DOE will accept final FCLs granted by CSAs for access to national security information (NSI). Upon acceptance of the reciprocity agreement from the CSA, DOE will not subject the contractor to any additional processing when:

(a) No proscribed information is involved, and

(b) The FCL is commensurate with the new safeguards and security activity.

(5) Notification of Cancellation. An assurance must be obtained from the CSA that the FCL will not be canceled prior to the CSO being notified.

(6) Protective Measures. Written confirmation must be obtained from the CSA that the facility's protective measures and procedures are adequate for the protection of the DOE activity, and results of the agency's last survey of the facility are satisfactory in those areas that could affect the DOE interest.

(7) Surveys. The facility's survey frequency must be confirmed by the CSA. For possessing (safeguarding) interests, the CSO must obtain the CSA's periodic survey reports or memoranda covering the survey results.

(8) Restricted Data (RD), Formerly Restricted Data, and Transclassified Foreign Nuclear Information (TFNI). When RD, FRD, or TFNI are involved, the following must be completed:

(a) An assurance must be obtained from the CSA that the facility complies with the requirements of 10 CFR Part 1045, *Nuclear Classification and Declassification*.

(b) When the DOE contract involves RD, an assurance must be obtained from the CSA that the facility's protective measures and procedures meet the requirements of 32 CFR 117, *National Industrial Security Program Operating Manual (NISPOM),* including any additional requirements applicable to RD, or negotiated between CSAs.

Must ensure that all associated DOE requirements established in the current versions of DOE O 471.6, *Information Security,* DOE O 452.8 *Control of Nuclear Weapon Data*, and/or other requirements established by the data owners, are met.

(c) FCLs not meeting the requirements in (a) and (b) above may be accepted when the DOE activity requires that the contractor establish upgraded protective measures that meet DOE requirements. For FCL upgrades, the agreement between DOE and the CSA must cover reimbursement for upgrade costs incurred by the CSA or contractor.

(d) When DOE accepts an FCL based on a CSA-approved Voting Trust Agreement, Proxy Agreement, SSA, or SCA, an assurance must be obtained from the CSA that it will invite and permit DOE to attend the annual meeting when such attendance is determined necessary by either the CSA or DOE.

(9) Contractor's Tier Parent(s).

(a) If the parent(s) of a company that DOE is processing for an FCL holds an FCL granted by a CSA, the tier parent(s) does not need to provide DOE with a FOCI package, provided reciprocity is accomplished with the CSA.

(b) Reciprocity between the CSO and the CSA must be documented in a written agreement with the appropriate provisions as outlined above.

(c) The written agreement must contain an assurance from the CSA that security cognizance will be transferred to DOE for any tier parent no longer requiring the CSA's FCL.

b. CSA Verification Requests. When a CSA requests verification of an existing DOE FCL, a copy of the facility's current FDAR, must be provided.

ATTACHMENT 2
SECTION 5: DOCUMENTATION AND REGISTRATION OF FCL AND RELATED SECURITY ACTIVITIES

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL.

   a. More than one Departmental element may register a security activity for an entity. The CSO with the highest security classification level and category of the security activity will maintain cognizance of the entity.

   b. When a contractor entity has a contract performance with a lower security classification level, but has a possessing security activity requirement, the CSO for the possessing contract performance will retain cognizance of the contractor. This responsibility may be delegated, by mutual agreement, to another Departmental element with a registered security activity at that facility.

   c. Any change in the responsible CSO or survey office must include a transfer of appropriate documentation (e.g., safeguards and security (S&S) plans; construction project status; FOCI files; etc.) and must be recorded on the FDAR.

2. REQUIREMENTS.

   a. FCL Documentation.

      (1) SSIMS must be used by all CSOs to register FCL information for which they have cognizant security authority, survey cognizance, or responsibility for registered security activities. Each registered FCL must identify the highest security activity approved for the registered facility.

      (2) DOE F 470.1, *Contract Security Classification Specification (CSCS)* is used to register information in SSIMS concerning all contract vehicles requiring PCLs in the performance of the work. Each contract must have a unique CSCS form in SSIMS.

      DD FORM 254, *Department of Defense Contract Security Classification Specification*, used by a CSA sponsoring an activity can be submitted in lieu of the DOE F 470.1, CSCS. For entry into SSIMS, the information will need to be transferred onto DOE F 470.1.

      (3) DOE F 470.2, Facility Data and Approval Record (FDAR) is used to record approvals, changes, and terminations of FCL security information and other facility changes for entry into SSIMS.

   b. Registration of Security Activities. Security activities are specific, unrelated tasks

or contract elements involving S&S interests at a facility. Security activities must be registered in association with a specific FCL.

c. Federal Contracting Office. For contracts awarded by a federal contracting office, the procurement request originator must submit a DOE F 470.1, *CSCS*, or DD FORM 254 *Department of Defense Contract Security Classification Specification*, to the DOE contracting official, who must forward the completed DOE F 470.1 to the CSO.

d. Prime Contractor. For contracts awarded by a contractor, the prime contractor must submit a DOE F 470.1, *CSCS*, to the CSO.

e. Security Activities for Existing FCLs. The CSO must:

(1) Determine and validate all security requirements for the proposed security activity.

(2) Determine the FCL status through SSIMS.

(3) Compare the security requirements for the activity to the approved FCL in the following situations and ensure that:

(a) When the contractor FCL is granted by a CSO, the requirements for accepting an FCL are met.

(b) When the contractor FCL is granted by DOE:

1 The new activity will be protected adequately under the facility's existing S&S program as outlined in the facility's approved security plan.

2 The existing FCL is compatible with the level and category of the new security activity.

3 The facility holds an overall composite satisfactory facility rating in the last S&S survey report.

f. New Security Activities.

(1) The CSO must verify the information and ensure that the new security activity can be performed within the existing FCL. If no issues are identified, the CSO will approve the FDAR and CSCS, as appropriate and ensure that it is registered in SSIMS.

(2) When a new activity exceeds the current FCL, or if there is no FCL, all actions required to upgrade the current level or obtain an FCL must be completed prior to contract award.

g. Modifying Security Activities.

(1) When a security activity is modified (e.g., period of performance, scope of work, classification level/category, place of performance, etc.), a revised CSCS must be submitted to the CSO.

(2) The CSO must verify the information and ensure that the new security activity can be performed within the existing FCL. If no issues are identified, the CSO should approve the CSCS and must ensure that it is updated in SSIMS.

(3) When a modified activity exceeds or reduces the current FCL needs, all actions required to upgrade, downgrade, or terminate the current FCL must be completed.

h. Strategic Partnership Projects (SPP) Activities.

(1) SPP security activities are registered in SSIMS, or the SPP agreements must be available in a locally approved system and must comply with the requirements of DOE O 481.1, *Strategic Partnership Projects* [Formerly Known as Work for Others (Non-Department of Energy Funded Work)], and DOE O 475.2, *Identifying Classified Information,* current versions.

(2) SPP Performed at Other Than DOE-Owned or DOE-Operated Facilities.

(a) When a CSA stipulates that SPP activities are to be performed by a DOE contractor at locations other than DOE-owned or DOE-operated facilities, an FCL is required.

(b) When the FCL is issued by a CSA, the requirements for accepting CSA FCLs apply.

(3) Subcontracting in Connection with SPPs.

(a) A CSA SPP FCL will be established based on a reciprocity agreement between the CSO and the CSA.

(b) SPP facilities do not require DOE clearances; therefore, the CSA will remain responsible for all security aspects to include FOCI, KMP clearances, surveys, etc., as outlined in the reciprocity agreement.

(c) A CSCS is required and must be registered in SSIMS under the CSA FCL as an OGA Contractor - Strategic Partnership Projects.

i. Special Access. Access to the categories below is limited to personnel who are properly briefed and require access to the information, equipment, and/or materials to perform the duties associated with the security activity. Contractor access to the categories below must be recorded on DOE F 470.1.

(1) Sensitive Compartmented Information (SCI) must be selected on the DOE F 470.1 when a security activity requires access to classified information concerning or derived from intelligence sources, methods, or analytical processes that must be handled within formal access control systems established by the Director of National Intelligence.

(a) The Special Security Officer, Office of Intelligence and Counterintelligence must provide prior approval of the DOE F 470.1 before a subcontract involving access to intelligence information can be issued to the subcontractor.

(b) The Field Intelligence Element Special Security Officer or Alternate Special Security Officer must sign the DOE F 470.1 for security activities involving access to SCI.

(2) Communications Security (COMSEC) must be selected on the DOE F 470.1 when:

(a) The security activity requires access to accountable, non-accountable COMSEC and controlled cryptographic items (CCI).

(b) If a COMSEC account will be required, the DOE F 470.1 must contain a statement in the classification guidance section regarding the establishment of a COMSEC account. Reference current DOE O 470.6, *Technical Security Program,* current version, for additional COMSEC information and requirements.

(3) Select Critical Nuclear Weapon Design Information (CNWDI) on the DOE F 470.1 when applicable.

(4) Nuclear Weapon Data (NWD)/Sigma.

(a) NWD/Sigma must be selected on the DOE F 470.1 when a security activity requires access to Nuclear Weapon Data and Sigma Categories14, 15, and 20.

(b) Access to NWD and Sigma Categories are authorized only for TS/RD, TS/FRD, S/RD, and S/FRD facilities.

(c) Refer to DOE O 452.8, *Control of Nuclear Weapon Data,* current version*,* for requirements for authorizing NWD and Sigma access.

(d) When Sigma 14 or 15is requested, the site Use Control Site Coordinator must provide approval of each security activity (i.e., CSCS) prior to registration in SSIMS.

(e) When Sigma 20 is requested, the Sigma 20 Site Coordinator must provide approval of each security activity (i.e., CSCS) prior to registration in SSIMS.

(f) North Atlantic Treaty Organization Information (NATO) must be selected on the DOE F 470.1 when a security activity requires access to classified information or documents belonging to NATO or containing NATO classified information.

(g) Special Control Markings. Some classified matter may include special control markings that impose additional handling and dissemination limitations and/or describe the type of information involved.

(5) Foreign Government Information (FGI).

(a) Verify with the CSA that the prospective subcontractor has the appropriate FCL, classified information storage capability and review the prime contract to determine if there are any contractual limitations for approval before awarding a subcontract.

(b) Provide appropriate security FGI classification guidance and incorporate the pertinent security provisions on the DOE F 470.1.

j. Exceptions to SSIMS Registration. Details concerning sensitive or classified activities, the publication of which in SSIMS would compromise mission completion, are not registered in SSIMS. Foreign intelligence information, SCI, SAPs, and other sensitive activities requiring special access or procedures associated with receipt, storage, processing, and/or handling must conform to the applicable protection provisions of Executive Orders and to applicable Intelligence Community Directives. Exceptions to the registration requirements are identified below.

(1) SAPs. SAPs are not registered in SSIMS. SAPs are registered in accordance with DOE O 471.5, *Special Access Programs*, current version.

(2) SCI. SCI Security Programs are not registered in SSIMS; however, each accredited SCI facility (SCIF) must be recorded in SSIMS using DOE F 470.2, Facility Data and Approval Record (FDAR).

Note: The registration of classified or sensitive details must not be entered into SSIMS.

ATTACHMENT 2
SECTION 6: INTERIM AND LIMITED FCLS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. INTERIM FCL. The DOE cognizance security office may grant an interim FCL on a temporary basis, pending the completion of full investigative requirements for KMP personnel security clearances.[10]

    a. Interim FCLs will only be granted when KMP personnel security clearances are pending with the Cognizance Personnel Security Office (CPSO).

        (1) All other eligibility requirements (e.g., favorable FOCI determination, approved security plans, satisfactory survey, as applicable) must be finalized prior to the grant of an interim FCL.

        (2) Interim FCLs must be registered in SSIMS.

    b. When final personnel security clearances have been granted to all personnel required to be cleared in connection with the FCL, a final FCL must be granted and registered in SSIMS via an updated DOE F 470.2, *Facility Data and Approval Record (FDAR)*.

    c. When a KMP personnel security clearance is withdrawn, suspended, cancelled, or terminated, the interim FCL must also be suspended. The FCL cannot be converted back to active status until the new KMP is in process or granted.

    d. Contractors under FOCI or those with foreign nationals as KMP are not eligible for interim FCLs.

2. LIMITED FCL. The United States has entered into agreements with certain foreign governments that establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negation or mitigation instrument. Limited FCLs ensure that the release of information or access to security assets is in accordance with the U.S. National Disclosure Policy.

    a. A limited FCL must be restricted to one security activity involving classified information or DOE security assets.

    b. Award another security activity to the same facility involving such information requires a separate FCL registration under another limited FCL, or under an FCL

[10] "Interim FCLs" are also known as "Temporary FCLs" and may be used interchangeably within other NISP Agencies.

without restrictions, if appropriate.

c. Issuance of a limited FCL requires that strict access restrictions must be imposed to limit the access to the scope of the contract.

d. Limited FCLs are granted solely at the discretion of DOE upon satisfaction of all criteria and requirements.

(1) All FCL approval requirements apply to a limited FCL.

(a) Verification of an agreement authorizing the exchange of the classified information or matter involved to the country from which the foreign ownership is derived.

(b) Access to classified information or matter will be limited to performance on a contract, subcontract, or program involving the government of the country from which foreign ownership is derived.

(c) Release of classified information or matter must be in conformity with the U.S. National Disclosure Policy.

(2) In extraordinary circumstances, a limited FCL may be granted when the criteria listed above cannot be satisfied, provided there exists a compelling need to do so consistent with national security interests.

(3) Limited FCL Compelling Need Statement. Each request for clearance under a limited FCL must be accompanied by a statement of compelling need from the GCA.

(a) The GCA's compelling need statement must be signed by the head of the cognizant DOE program office and include the following:

1 Acknowledgment that the company will be under FOCI (i.e., FOCI will not be mitigated).

2 Acknowledgment that the GCA/Departmental element accepts the risks inherent in the

3 granting of an FCL where FOCI is not mitigated.

4 A foreign disclosure determination stating the basis for determining that release of classified to the foreign government involved is in conformity with U.S. National Disclosure Policy.

ATTACHMENT 2
SECTION 7: FACILITY CLEAREANCE SUSPENSIONS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. REASONS FOR SUSPENSION. The CSO, in coordination with the ODFSA, must suspend the FCL and register the suspension in SSIMS when the following conditions occur:

   a. A contractor is determined to be under FOCI that has not been mitigated, the FCL must be suspended. Contract performance on activities involving proscribed information must not continue until all applicable FOCI requirements are met.

   b. Findings or other deficiencies in a survey, self-assessment, inspection, or evaluation indicate suspension of a FCL is necessary due to non-compliance with FCL or other requirements.

      (1) The CSO will determine if the FCL must be suspended pending validated corrective actions.

      (2) The prime contractor may recommend the CSO suspend the FCL of a contractor under their cognizance.

   c. Any required KMP that is not cleared at the level of the FCL.

      (1) Once the KMP is verified to be in process with the CPSO, the FCL may be registered as an Interim FCL.

      (2) When the KMP clearance is granted, the FCL can be registered as a final.

   d. A CSA or CSO invalidates or suspends the FCL issued under its cognizance.

   e. Noncompliance with security and reporting requirements.

   f. Mergers/Acquisitions that impact the cleared contractor's business structure, operations, and/or work involving security activities and/or assets.

2. ACTIONS. The CSO, in coordination with the ODFSA, must take the following actions when it suspends a contractor's FCL:

   a. Notify the contractor, in writing, that its FCL has been suspended. Notification must include:

      (1) The reason for the suspension, required corrective actions, and associated timeline, and provisions for current contract extensions.

      (2) Award of new contracts to the facility will not be permitted until the

facility has been restored to a fully valid status.

(3) Except for KMP, as designated by the CSO, no new personnel security clearances may be requested or processed.

(4) Termination of the FCL may result if the issues causing the suspension, as identified by the CSO, in the written notification are not rectified within the time frame and manner specified; and

(5) For possessing facilities, the suspension notification must include instructions for securing security assets at an approved cleared facility.

(6) Contractors must take immediate action to implement these instructions.

b. Notify the GCA of the suspension.

(1) The GCA must make the final decision to continue the contractor's performance on existing contracts.

(2) The ODFSA must evaluate the contractor's security program to ensure security assets that remain in the contractor's possession are protected.

c. Notify all affected DOE elements and applicable CSAs of the suspension.

3. NONCOMPLIANCE WITH MITIGATION PLANS. When the CSO determines that a cleared contractor or its tier parent is out of compliance with an approved FOCI mitigation plan, the CSO will analyze and evaluate the overall impact to the protection of security interests. The CSO must take the appropriate actions:

a. Notify the cognizant contracting officer immediately.

b. Request a corrective action and implementation plan from the contractor to bring it into compliance with the approved mitigation plan. The contractor must immediately supply the plan and all related information upon request

c. Suspend the FCL. The CSO must ensure contractors immediately comply with all instructions from the CSO pertaining to the suspension.

d. Terminate the FCL. When the CSO terminates a contractor's FCL, the contractor must immediately comply with instructions and termination requirements set forth in Section 8 of this Attachment.

4. <u>CONTINUATION OF CONTRACT PERFORMANCE UNDER FOREIGN GOVERNMENT OWNERSHIP</u>. In accordance with the intent of 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition*, when an existing contractor becomes foreign government owned, but execution of a novation agreement is not required by the DEAR, the continued performance by that contractor on existing classified contracts or contracts for

environmental restoration, remediation, or waste management that involve proscribed information may only continue under FCL suspension if:

a. The contractor is eligible for continuation on such work by Secretarial and/or CSA Secretarial waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable.

b. Each GCA takes immediate action to request a waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable.

c. Appropriate actions are taken to safeguard the security assets.

5. REINSTATEMENT OF A SUSPENDED FCL. The CSO may reinstate the FCL when the conditions that resulted in the suspension are resolved. The reinstatement must be based on the necessity to complete or continue work associated with the original FCL.

ATTACHMENT 2
SECTION 8: SECURITY ACTIVITY/FCL TERMINATION

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. SECURITY ACTIVITY TERMINATION.

   a. When a security activity ends, the CSO and/or ISSP must enter a final DOE F 470.1, *Contract Security Classification Specification (CSCS)*, into SSIMS to reflect the termination of each security activity.

   b. If other registered security activities exist, CSOs and/or ISSPs must follow the "Transferring FCL Cognizance" requirements in Section 2 of this Attachment.

   c. Non-Possessing Facilities. Upon termination of each security activity, the contractor must submit a certification certifying that all personnel security clearances connected with the contract have been transferred to another contract under the same Facility Code or terminated within 30 days.

   d. Possessing Facilities. Upon return, reallocation, disposition, or destruction of all classified matter pertaining to a security activity, the contractor must submit a certificate of non-possession to the CSO. The certificate must include the contract number and a statement that all classified matter has been returned to authorized representatives of DOE or destroyed.

      (1) Upon termination of each security activity, the contractor must submit a certification certifying that all personnel security clearances connected with the contract have been transferred to another contract under the same Facility Code or terminated.

      (2) For security activities involving special accesses (SCI, SAP, COMSEC, etc.), the respective office must take action to ensure that all classified interests have been appropriately dispositioned.

      (3) Contractors are not permitted to retain SNM/OANM.

      (4) Certificate of Possession must:

         (a) Describe DOE's benefit and the contractor's intended use of the information.

         (b) Identify the specific classified matter by subject, type or form, and quantity.

         (c) State that the classified matter will retain its initial classification until downgraded or declassified by DOE.

(d) Certify that security assets will be safeguarded in accordance with DOE requirements.

1 The contractor must immediately report potentially compromised and/or unaccounted for security assets to the CSO, and

2 Acknowledge that unauthorized disclosure of classified matter is subject to criminal penalties.

(5) All requests to retain security assets must be provided to the CSO for approval prior to the termination of the security activity.

(a) The CSO must notify the contractor, in writing, of the decision.

1 If the security assets will aid the contractor in performing another active government contract and the matter is being transferred to the active contract, the contractor must provide the CSO and the CSA holding the contract a copy of the retention notification.

2 If the contractor does not receive the required notification, the matter may be transferred and will fall under the jurisdiction of the gaining (i.e., active) contract.

(b) When a certificate of possession is submitted, the contractor may maintain the security assets for up to 24 months, unless otherwise notified by the CSO having authority over the security assets.

For classified matter belonging to another CSA, the CSO must obtain concurrence from the CSA.

2. FCL TERMINATION.

a. When the last security activity ends and/or an FCL is no longer necessary, the FCL must be terminated.

b. Prior to termination, the CSO must:

(1) Ensure all personnel security clearances connected to the FCL are terminated.

(2) Ensure all DOE security assets are appropriately reallocated, disposed of, destroyed, or returned to an authorized DOE Federal or contractor with the appropriate FCL level.

c. For Possessing facilities, the CSO must complete a termination survey; and

d. An updated DOE F 470.2, *Facility Data and Approval Record (FDAR)* must be entered into SSIMS to reflect the termination.

3. REACTIVATION. Reactivations of terminated FCLs must be based on programmatic or mission need and the implementation of current security requirements.

a. The CSO must:

(1) Validate that all security requirements (e.g., FOCI, KMP personnel security clearances, etc.) have been implemented,

(2) Must complete a DOE F 470.2, Facility Data and Approval Record (FDAR), and

(3) Must update SSIMS to complete the reactivation.

ATTACHMENT 3
FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL.

   a. Foreign investment plays an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States.

   b. The DOE Foreign Ownership, Control, or Influence (FOCI) policy for U.S. companies subject to a facility clearance (FCL) determination is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology and/or classified information or matter, including RD, FRD, and SNM/OANM.

   c. The FOCI program regulates DOE determinations of the degree to which a contractor facility is under foreign ownership, control, or influence. In accordance with 48 CFR Chapter 9, the DOE Acquisition Regulation (DEAR), DOE must obtain information about FOCI that is sufficient to help the Department determine whether award of a contract to a person or firm, or the continued performance of a contract by a person or firm, may pose undue risk to the common defense and security.

   d. A contractor cannot be under FOCI to such a degree that granting or continuing an FCL would be inconsistent with U.S. national security interests. The requirements of the National Industrial Security Program (NISP) form the baseline for this program, supplemented with requirements for the protection of DOE-specific assets, Restricted Data, SNM/OANM, and other security activities.

2. REQUIREMENTS.

   a. Cognizant Security Office (CSO). The CSO and/or the Industrial Security Service Provider (ISSP)[11], as designated by the Program Secretarial Officer or, for NNSA, the Office of the Administrator through the Office of Defense Nuclear Security, must ensure that the following activities are accomplished under the FOCI program for facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the FOCI program must be documented in facility or site security plans.

[11] For the purposes of this Attachment, CSO and ISSP may be interchangeable to identify FOCI responsibilities.

b.

(1) Ensure FOCI determinations are rendered for all contractors and their tier parents as required.

(2) Establish and implement procedures to ensure coordination is accomplished between the FCL and FOCI programs.

(3) Ensure that all relevant aspects of FOCI are resolved and, if necessary, appropriately mitigated prior to the granting of an interim or final FCL.

(4) Establish reporting requirements and timelines for which contractors must report changes to the FOCI determination.

(5) Ensure that contractors under their cognizance meet reporting requirements as established in DOE directives and national standards.

(6) Establish and determine the circumstances under which a contractor will be requested to complete a new FOCI package.

(7) Ensure that contractors under FOCI mitigation comply with all requirements imposed by the mitigation instrument.

(8) Ensure that procedures are in place for verification of the original signature on the Standard Form (SF) 328, Certificate Pertaining to Foreign Interest, prior to finalizing a FOCI determination.

(9) Ensure that counterintelligence threat and technology transfer risk assessments and updates are obtained and evaluated as necessary in the administration of the FOCI program.

(10) Ensure that annual review and certification requirements or alternative methods as permitted by this Order, for contractors under a FOCI mitigation instrument, are met for all such contractors under their cognizance.

(11) Ensure that when factors not related to ownership are present, contractors take appropriate positive measures to assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on contracts.

(12) Approve trustees, proxy holders, and outside directors nominated by contractors in connection with FOCI mitigation plans and approve specific measures such as technology control plans developed and implemented by contractors as part of FOCI mitigation plans.

(13) Evaluate changes in FOCI information submitted by contractors holding an FCL, and make changes in mitigation methods or security

requirements, or suspend or terminate the FCL, as warranted to address changed conditions.

(14) Establish an appeals process for disputing a FOCI determination or National Interest Determinations (NIDs) non-concurrence.

c. Contractors. Contractors must ensure that the following activities are accomplished for the FOCI program. An FCL will not be granted until all relevant aspects of FOCI have been resolved and, if necessary, appropriately mitigated. Procedures applicable to the FOCI program must be documented in facility or site security plans.

(1) Establish and maintain activities related to FOCI in accordance with the requirements contained in this directive and in national policies.

(2) In all FOCI activities, provide complete information to enable the DOE cognizant security office and/or other DOE Federal authorities to ascertain the attendant risk and whether classified information and other security assets are adequately protected, including but not limited to accurate and complete submissions of Standard Form (SF) 328, Certificate Pertaining to Foreign Interest, and information provided during annual certification and review activities.

(3) Ensure changes reported by contractors which might affect the FOCI determination are reported, via e-FOCI to the respective DOE or NNSA cognizant security office and/or other DOE Federal authorities upon notification.

(a) Comply with all reporting requirements related to FOCI.

(b) Maintain all records pertaining to FOCI, including records such as original signatures on the SF 328 if instructed by the DOE cognizant security office, and make such records available upon request to the CSO.

(c) Complete a new FOCI package when directed to do so by the DOE cognizant security office or on a schedule established by that office.

(4) Propose appropriate FOCI mitigation instruments and work with the CSO to develop a suitable FOCI mitigation plan in accordance with national drivers and regulatory guidance.

(5) Comply with all requirements and restrictions imposed by an approved FOCI mitigation plan.

(6) Furnish annual review and certification information one year from the effective date of a mitigation agreement and annually thereafter.

(7) Complete required Facility Security Officer (FSO) and Insider Threat Program Senior Official training in accordance with Attachment 2 of this Order.

(8) When issues not related to ownership are present, take appropriate positive measures to assure that the foreign interest is effectively mitigated and cannot adversely affect security assets and performance on contracts.

(9) When FOCI is mitigated through use of a Voting Trust, Proxy Agreement, Special Security Agreement (SSA) or Security Control Agreement (SCA), establish a permanent committee of the organization's board of directors as the government security committee.

3. FOCI PROGRAM INFORMATION.

a. General.

(1) FCL must not be granted until all relevant aspects of FOCI have been resolved and, if necessary, appropriately mitigated. Appropriate procedures must be in place to ensure coordination between the FOCI and FCL programs under the jurisdiction of each DOE program office.

(2) The determination of whether a U.S. company is under FOCI must be made on a case-by-case basis. In instances where the company is unable to identify a foreign owner (e.g., the participating investors in a foreign investment or hedge fund cannot be identified), CSO may determine that the company is not eligible for an FCL. The following are examples of factors that must be considered to determine whether a company is under FOCI, is eligible for an FCL despite FOCI issues, and the protective measures required to mitigate FOCI:

(a) Foreign intelligence threat, including record of economic and government espionage against U.S. targets.

(b) Risk of unauthorized technology transfer.

(c) Type and sensitivity of classified information or matter, or SNM/OANM to be accessed.

(d) The nature, source, and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration all immediate, intermediate, and ultimate parent companies.

(e) Record of compliance with pertinent U.S. laws, regulations, and contracts.

(f) Nature of bilateral and multilateral security and information exchange agreements that may be relevant.

(g) Whether the government of the foreign interest has industrial security and export control regimes in place that are comparable to those of the United States.

(h) Ownership or control, in whole or in part, by a foreign government.

(3) Development of security measures to mitigate the impact of unacceptable FOCI must be based on the concept of risk management.

(4) If there is a change in a company with an existing FCL that impacts a favorable FOCI determination, the FCL must be suspended or terminated unless security measures are taken to remove the possibility of unauthorized access or adverse impacts to contract performance.

(5) Any doubt that unacceptable FOCI can be effectively mitigated to the point that affording the applicant access to classified information or matter is clearly consistent with national security must be resolved in favor of the national security.

b. Applicability.

(1) FOCI determinations must be rendered on the following:

(a) Applicants, including industrial, educational; commercial; or any other entity, grantee, or licensee that have or anticipate executing a contract requiring access authorizations, including individuals contracting as a business. This includes subcontractors of any tier, consulting firms, agents, grantees, and cooperative research and development agreement participants who require security clearances.

(b) All tier parents of applicants when the parent is located in the United States, Puerto Rico, or a U.S. possession or trust territory (DEAR, section 925.204-73[f]).

(2) A FOCI determination is not required for an individual performing work under a consulting agreement (e.g., an individual awarded a contract who has not contracted as a business). Foreign involvement for such individuals is determined and adjudicated through the background investigation conducted for the security clearance.

(3) When a local, State, or Federal agency or department is granted an FCL, there must be an agreement containing a security clause, which must state that if the government agency or department subcontracts any work requiring access to classified information or matter by a commercial entity

in connection with the FCL, a FOCI determination is required. If the government agency or department does not have its own FOCI policies or an agreement with the Secretary of Defense for industrial security services, DOE will render the FOCI determination.

(4) Contractors with existing U.S. Government FCLs are identified in SSIMS and/or Defense Counterintelligence and Security Agency National Industrial Security System. No further FOCI review is required for an applicant registered in either of these systems holding an equal or higher U.S. Government FCL based upon a favorable FOCI determination.

c. Electronic Submission/Processing Web Site. The Department has an electronic system for submission of FOCI information to DOE. To ensure confidentiality of the information submitted and stored on the system, the site is protected with 128-bit encryption.

(1) Applicants must use this system for the submission of FOCI packages, including changes to update their FOCI information. The FOCI Website may be accessed via an Internet browser at https://foci.anl.gov. Electronic signatures are not accepted; therefore, a signed original SF 328, Certificate Pertaining to Foreign Interests, executed in accordance with the instructions on the certification section of the SF 328, must either be submitted to the DOE cognizant security office, or retained by the applicant and inspected by the DOE cognizant security office at the applicant's place of business prior to rendering the final FOCI determination.

(2) Federal employees and supporting contractors must use the Electronic Submission Processing System Website at https://doefoci.anl.gov.

ATTACHMENT 3
SECTION 1: FOCI PROGRAM PROCESSING

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. FOCI PROCESSING.

   a. Determining the Requirements for a FOCI Determination. If the procurement request requires security clearances, the DEAR security clauses found at 48 CFR Part 952.204-2, *Security Requirements*, will be included in the contract. For all such contracts a DOE F 470.1, *Contract Security Classification Specification (CSCS)*, must be completed by the procurement request originator. A DD Form 254 may be used by a Federal agency sponsoring a contract activity, provided it is annotated with the DOE facility code. FOCI information and forms required under the security clauses will be submitted via the electronic FOCI website.

   b. Final FOCI Determinations.

      (1) When insufficient lead time is expected between selection and contract award for the processing of the FOCI determination, the contracting officer may request a cursory review, not a final FOCI determination, of the SF 328 submissions of each applicant in the competitive range.

      (2) A final FOCI determination will only be rendered for the successful applicant.

   c. Adjudication Level.

      (1) The DOE cognizant security office renders the FOCI determination under the following conditions:

         (a) The responses to the FOCI questions do not exceed the thresholds in the FOCI Implementation reference tool in the e-FOCI system.

         (b) Exclusion procedures are invoked when the applicant is controlled by a parent(s) not requiring security clearances or requiring a lower level of access to classified information or matter.

      (2) The Office of Environment, Health, Safety and Security (EHSS), or for NNSA, the Chief, Office of Defense Nuclear Security, will render FOCI determinations that exceed established thresholds. The DOE cognizant security office will forward the FOCI submission(s) to EHSS or NNSA with:

         (a) the justification for clearance or exclusion, including full details pertaining to the proposed contract, and

(b) the DOE cognizant security office's analysis, including a clear statement of the reason why a Headquarters determination is required. The Headquarters office, in coordination with the Office of General Counsel, will provide a final FOCI determination to the submitting office.

(3) A counterintelligence threat assessment and technology transfer risk assessment must be obtained and considered prior to a final decision to grant an FCL to an applicant under FOCI or to restore an FCL previously suspended because of unacceptable FOCI. The DOE cognizant security office must coordinate with the DOE Office of Intelligence and Counterintelligence (DOE/IN-21) to ensure that the threat assessment and technology transfer risk assessments and updates are accomplished.

d. Committee on Foreign Investment in the United States.

(1) The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee chaired by the Department of the Treasury under Section 721 of the Defense Production Act of 1950 (50 U.S.C. App. 2170). CFIUS review is a voluntary process which affords an opportunity for foreign investors and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on national security. DOE policy regarding CFIUS is found in DOE O 142.5, Committee on Foreign Investment in the United States, current version.

(2) The CFIUS review and the FOCI and FCL processing actions are carried out in two parallel but separate processes with different time constraints and considerations.

e. Contracting Officers. Contracting officers must provide electronic or written notification to the DOE cognizant security office when:

(1) they become aware of any changes to an applicant's FOCI status.

(2) a requested FOCI review is no longer needed.

(3) a FOCI determination was rendered on an applicant that was not awarded a contract.

(4) all work on a contract for which a FOCI determination was rendered is within 30 days before termination or completion; or

(5) security clearances are no longer required in performance of the contract.

ATTACHMENT 3
SECTION 2: FOCI REPORTING REQUIREMENTS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL. Contractors are required to report changes that have an impact on the status of the FCL. The reporting requirements stated here pertain specifically to the FCL; additional requirements related to FOCI issues, personnel security concerns, and other security matters are also reportable and can be found in the directives applicable to those programs.

2. UPDATES. Contractors holding an FCL must submit written reports of changed conditions and any anticipated changes affecting the FCL when the change or impending change is made known.

   a. Significant changes. When changes have occurred in the extent and nature of FOCI that affect the information in a contractor's most recent FOCI submission, the contractor must provide written notification and supporting documentation relevant to the changes to the CSO. Significant changes include but are not limited to the following circumstances:

      (1) All circumstances that would change any answer on the SF 328, *Certificate Pertaining to Foreign Interest,* from "No" to "Yes," must be reported by submitting a changed condition SF 328.

      (2) A previously reported threshold or factor that was favorably adjudicated by the CSO has increased to a level requiring a determination by the Office of Environment, Health, Safety and Security or, for NNSA, the Office of Defense Nuclear Security.

      (3) When a foreign interest owns five percent or more of a U.S. business organization (Questions 1a and 1b, SF 328), a five percent or greater increase in the beneficial ownership of a class of equity securities of the business organization, or a five percent increase in the beneficial ownership of the business itself, as determined by voting or investment rights, by one or more foreign interests and/or any U.S. person effectively controlled by a foreign interest.

      (4) When a U.S. business organization owns ten percent or more of a foreign interest (Question 2, SF 328), any increase equivalent to ten percent or more of the tangible net worth of the business organization.

      (5) When a U.S. business organization has foreign national Key Management Personnel (KMP) (Question 3, SF 328), appointment of any additional foreign national to a position required to be cleared in connection with the FCL or to any position identified in the articles of incorporation, by-laws,

articles of organization, or equivalent governance documentation or charter for the business organization.

(6) When a Foreign Person has the power to control selection or tenure of KMP/other decisions (Question 4, SF 328), any change in such power/authority except amendments or waivers to governance documentation either to correct manifest error or which are of a formal, minor, or technical nature and do not change materially any person's rights or obligations.

(7) When there are contracts, agreements, understandings, or arrangements with foreign person(s) (Question 5, SF 328), any change expected to result in annual payments to or from an entity where the payments exceed twenty percent of the U.S. business organization's annual gross revenues.

(8) When there is indebtedness, liabilities, or obligations to foreign persons (Question 6, SF 328), there is a changed condition reportable on the SF 328 whenever there is:

(a) Any new indebtedness to foreign persons which results in a liability exceeding ten percent of the tangible net worth of the business organization or includes an instrument creating a mortgage, deed of trust, pledge, lien, security interest or other charge or encumbrance against:

1 Any of its property, assets or leasehold interests exceeding ten percent of the business organizations tangible net worth, or

2 Pledges five percent or more of the voting securities of the business organization as collateral.

(b) Any other new foreign indebtedness where the business organization permits to exist a leverage ratio exceeding two to one (2:1) based on the business organization's indebtedness to its tangible net worth and calculated on the basis of information set forth in its financial statement.

(9) When the business organization derives five percent or more of total revenues/net income from a single foreign person (Question 7a, SF 328), with respect to the business organization and that single foreign person, any change expected to result in annual payments to or from the business organization where the payments exceed an additional ten percent of the business organization's gross revenues.

(10) When the business organization derives thirty percent or more of total revenues/net income from foreign persons (Question 7b, SF 328), with respect to the business organization and any foreign persons, any change expected to result in annual payments to or from the business organization where the payments exceed an additional twenty percent of the business organization's annual gross revenue.

(11) When there are ten percent or more voting securities held in a method which does not identify the beneficial owner (Question 8, SF 328), any change of five percent or more in the total number of shares held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner or any amendment to the bylaws of the business organization or its parent related specifically to voting rights of such nominee holders and any requirement regarding notice of any matter to be presented by a nominee stockholder at a shareholders meeting including any amendment affecting the voting and notice rights and obligations of nominee holders and associated persons who fail to make timely disclosures required by the U.S. Securities and Exchange Commission (SEC) such as Schedule 13D.

(12) When there are KMP(s) holding positions or serving as consultants for foreign person(s) (Question 9, SF 328), any new position held by persons required to be cleared in connection with the FCL (excludes positions where the KMP is appointed by the U.S. parent business organization to a seat on the board or similar governing body of a foreign subsidiary, provided that the business organization promptly gives the CSO notice of such appointment).

(13) When there are any other factors of foreign person control or influence (Question 10, SF 328), each change qualifying as an affirmative answer to this question on the SF 328 and each change having a material effect on the ownership, control or influence of the business, operations, prospects, condition (financial or otherwise), or property of the business organization such that the security measures contemplated by an agreement with DOE to mitigate FOCI would not reasonably be expected to remove the possibility of unauthorized access to or adverse effect on the performance of classified contracts.

(14) A previously reported foreign ownership threshold or factor that was favorably adjudicated has increased to the extent that a FOCI mitigation method (if none previously existed) or a different FOCI mitigation method is required.

(15) Any changes in ownership or control, including stock transfers that affect control of the company. Notice of changes includes ownership or control events that are required to be reported to the SEC, the Federal Trade Commission, or the Department of Justice.

b. Anticipated changes. Anticipated changes are events that arise when the contractor or any of its tier parents enter into formal negotiations toward agreement or acquisition, e.g., when the parties enter a written memorandum of understanding); in the case of financing agreements, or when written application for financing is made. The contractor must provide the CSO with written notification of anticipated actions, including but not limited to the following:

(1) An action to terminate business or operations of the contractor or any of its parents for any reason, including but not limited to entering into any transaction of merger, consolidation, or amalgamation with another company; conveying, selling, leasing, transferring, or otherwise disposing of all or a substantial part of company business or assets; and/or making any material change that could have an adverse effect on the contractor organization's ability to perform its contractual obligations for DOE or other contractors of DOE.

(2) Legal actions taken to initiate bankruptcy proceedings involving the contractor organization or any of its tier parents.

(3) Imminent adjudication of/or reorganization resulting from bankruptcy actions involving the contractor organization or any of its tier parents.

(4) Entry by the contractor or its tier parents into negotiations with foreign nationals that may reasonably be expected to require amendment of the SF 328, including but not limited to negotiations for the sale of securities to a foreign national or citizens.

3. OTHER REPORTABLE CHANGES.

a. Changes to name or address of the company or any of its cleared locations.

b. Any changes to information previously submitted for KMP, including, if appropriate, the names of the individuals they are replacing. In addition, a statement including the following information must be provided to the CSO:

(1) Date and place of birth, social security number, citizenship, and, if appropriate, personnel security clearance level and issuing agency.

(2) If they have been excluded from access to security assets.

(3) If they have been temporarily excluded from access to security assets pending the granting of the DOE access authorization.

c. A new complete listing of KMP will be submitted to the CSO upon request.

d. Any pre-contract negotiation or award not placed through a government contracting activity that involves or may involve the release or disclosure of U.S. security assets to a foreign interest or access to classified information furnished by a foreign interest.

e. Contractors must provide a current list of all classified contracts and classified subcontracts issued to other contractors upon request.

f. Contractors must provide security costs charged to the government upon request.

g. The data points will be used by the DOE in developing the annual Report to the Director, Information Security Oversight Office.

ATTACHMENT 3
SECTION 2, CHAPTER 1: CHANGES TO FOCI INFORMATION

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

4. CHANGES TO FOCI INFORMATION.

a. FOCI changes that occur following submission of an SF 328 and before contract award. When an applicant has submitted a comprehensive FOCI package to the contracting officer and changes have occurred in the FOCI of the company prior to contract award, the applicant must submit an updated SF 328 and associated documents within the timeframe established by the CSO. DOE cognizant security offices must review the updated information and take any necessary steps to resolve FOCI concerns before the contract is awarded.

Failure to provide timely updates to the CSO may result in suspension of the FCL.

b. Updates. Changed conditions, such as a change in ownership, indebtedness, or foreign intelligence threat, justify adjustments to the security requirements under which a company is operating or require that a different FOCI mitigation method be used.

(1) A changed condition may result in a determination that a company is no longer considered to be under FOCI or, conversely, that a company is no longer eligible for an FCL.

(2) Contractors holding an FCL based upon a favorable FOCI determination must submit written reports of changed conditions and anticipated changes which affect the FCL.

(3) Changes must be analyzed by the DOE cognizant security office to ensure that the contractor continues to meet the standards for holding an FCL.

(4) DOE cognizant security offices may request updated information, including the submission of a new FOCI package, at any time outside the normal cycle of package submission requirements.

(5) Significant changes that warrant a new FOCI determination include the following:

(a) A new threshold or factor exists that did not exist when the previous determination was made.

(b) A previously reported threshold or factor that was favorably adjudicated by the DOE cognizant security office has increased to a level requiring a determination by EHSS or NNSA.

(c) A previously reported financial threshold or factor that was favorably adjudicated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location, end user, or lenders.

(d) Previously reported foreign ownership threshold or factor that was favorably adjudicated has increased to the extent that a FOCI mitigation method or a different FOCI mitigation method is required.

(e) Any changes in ownership or control, to include partnerships and joint ventures.

(f) Incidents of counterintelligence interest or concern identified and reported to the cognizant security office by the servicing counterintelligence office after the initial FOCI determination may also warrant a new determination.

c. Annual Review and Certification. The DOE cognizant security office will develop procedures to ensure that contractors provide adequate information to enable the DOE office to conduct a meaningful evaluation of compliance with annual review and certification requirements. Each contractor holding an FCL under a FOCI mitigation instrument must provide written annual certification to the DOE cognizant security office that no changes have occurred which would impact the contractor's ability to protect classified information or matter or otherwise impact to national security.

(1) The certification report must include:

(a) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement.

(b) Changes to security procedures, implemented or proposed, and the reasons for the changes.

(c) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of steps that were taken to prevent such acts from recurring.

(d) Any changes or impending changes of key management personnel or key board members, including the reasons for the changes.

(e) Any changes or impending changes in the organizational structure or ownership, including any acquisitions, mergers, or divestitures.

Any other issues that could have a bearing on the effectiveness of the applicable agreement. Any contractor controlled by a parent organization(s) that has/have been excluded by formal resolution

must provide written certification on an annual basis to the DOE cognizant security office acknowledging the continued effectiveness of the resolution.

(2) Any contractor that has executed a Board Resolution to reduce FOCI in non-controlling foreign ownership situations must provide annual written certification to the DOE cognizant security office acknowledging that the resolution remains in effect.

(3) Representatives of the DOE cognizant security office must meet annually (at least every 12 months) with the senior management officials who comprise the Government Security Committee (GSC) of organizations operating under a Voting Trust Agreement, Proxy Agreement, SSA, or SCA to review the effectiveness of the pertinent security arrangement and to establish a common understanding of the operating requirements and their implementation.

(a) If annual meetings cannot be conducted, CSO must establish other methods, such as the submission of a new FOCI package for review, to accomplish the same ends. Reviews must include examination of the following:

1 acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations.

2 problems or impediments associated with the practical application or utility of the security arrangement; and

3 whether security controls, practices, or procedures warrant adjustment.

ATTACHMENT 3
SECTION 3: PERSONNEL SECURITY CLEARANCES AND EXCLUSION PROCEDURES

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. SECURITY CLEARANCES REQUIRED IN CONNECTION WITH THE FCL.

   a. KMP, as determined by the CSO, must be cleared to the level of the FCL, or higher or formally excluded from access, as appropriate.

   b. For MFOs, each subordinate cleared facility's KMP must also be cleared or excluded.

   c. KMP PCL package requests must be submitted to the CPSO within established timelines, not to exceed 90 calendar days of notification. Failure to submit KMP PCL package requests to the CPSO may result in an FCL suspension or withdrawal.

2. EXCLUSION PROCEDURES. Certain contractor entity officials, e.g., those who either hold majority interest or stock in the entity, or who have direct or indirect authority to influence or decide issues affecting the management or operations of the contractor or classified contract performance, may be excluded from, or cleared at a lower level than the FCL. The CSO must ensure the following exclusion actions are completed before granting an FCL. Exclusion actions must be documented by the organization's governing board. A copy of the resolution must be provided via e-FOCI and approved by the CSO.

   a. When a formal exclusion action is required, the organization's governing body must determine the required exclusion action and make the appropriate affirmation:

      (1) Affirmation for Exclusion from Access to Classified Information:

         (a) Identify the KMP by their name and position to be excluded, will not require, will not have, and can be effectively and formally excluded from, access to all classified information disclosed to the entity, and

         (b) Does not occupy a position that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

(2) Affirmation for Exclusion from Higher-level Classified Information

(a) Identify the KMP by their name and position to be excluded, will not require, will not have, and can be effectively and formally excluded from access to classified information, and

(b) Does not occupy a position that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

3. SECURITY CLEARANCES CONCURRENT WITH THE FCL.

a. Contractor employees who are not KMP but will perform work on the contract may be submitted for PCLs concurrent with the submittal of the FCL request.

b. The PCL cannot be granted until the interim, limited, or final FCL is registered in SSIMS.

ATTACHMENT 3
SECTION 4: FOCI MITIGATION

1. FOCI MITIGATION.

a. General. If DOE determines that a company is under FOCI, DOE will determine the extent and manner in which the FOCI may result in unauthorized access to classified information or SNM/OANM and the types of actions that will be necessary to mitigate the associated risks to a level deemed acceptable in accordance with national drivers and DOE Policy. DOE cognizant security offices will ensure that the following are considered in every FOCI evaluation:

(1) Record of economic and government espionage against U.S. targets.

(2) Record of enforcement and/or engagement in unauthorized technology transfer.

(3) Record of compliance with pertinent U.S. laws, regulations, and contracts.

(4) Type and sensitivity of the information to be accessed.

(5) Source, nature, and extent of FOCI, including but not limited to whether foreign persons hold a majority or substantial minority position in the company, taking into consideration all immediate, intermediate, and ultimate parent companies.

(6) Nature of any bilateral and multilateral security and information exchange agreements that may pertain.

(7) Ownership or control, in whole or in part, by a foreign government.

(8) Any other factor that indicates or demonstrates a capability on the part of the foreign interests to control or influence the operations or management of the business organization concerned.

b. Mitigation Action Plans. If there are any affirmative answers on the Certificate Pertaining to Foreign Interests, or other information is received which indicates that the applicant may be under FOCI, the DOE cognizant security office must review the case to determine the relative significance of the information regarding the following factors:

(1) Whether the applicant is under FOCI.

(2) The extent and manner the FOCI may result in unauthorized access to classified information or adversely impact classified contract performance.

The type of actions, if any, that would be necessary to mitigate or negate the effects of the FOCI to a level deemed acceptable to the Federal Government.

FOCI Mitigation Instruments. The affected organization or its legal representatives may propose a plan to negate or reduce unacceptable FOCI.

(3) DOE must impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information or matter, or SNM/OANM, is precluded.

(4) An entity that will not implement the security measures determined necessary by DOE to mitigate its foreign involvement to an acceptable level is ineligible for a FOCI determination and an FCL.

(5) Under all methods of FOCI mitigation, management positions requiring security clearances in conjunction with the FCL must be filled by U.S. citizens residing in the United States.

c. Secretarial Waiver Authority. In accordance with 10 U.S.C. Section 2536, a contract under a national security program must not be awarded to an entity controlled by a foreign government if it is necessary for the entity to be given access to proscribed information until a waiver has been granted by the Secretary concerned (i.e., the Secretary of Energy or the Secretary of Defense).

(1) Secretarial waivers granted under 10 U.S.C. Section 2536(b)(1)(B) for an environmental restoration, remediation, or waste management contract, the Secretary must notify Congress of this decision.

(2) The contract may be awarded or the novation agreement executed only after the end of a 45-day period, beginning on the date notification is received by the Senate Committee on Armed Services and the House Committee on National Security.

d. Foreign Ownership. A controlling foreign ownership is one in which a foreign national(s) owns a majority of the voting securities of the U.S. organization or, if less than 50 percent is foreign owned, it can be reasonably determined that non-U.S. citizens or their representatives are in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from majority foreign ownership or control, a FOCI mitigation plan may consist of one of the following methods:

(1) Voting Trust Agreement. Under this type of agreement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government.

(a) Foreign owners must transfer legal title of the company to the Trustees.

(b) The Voting Trust Agreement does not impose any restrictions on the organization’s eligibility to have access to classified information or matter or to compete for classified contracts.

(c) A Government Security Committee (GSC) must be established under the Voting Trust to oversee classified, SNM/OANM, and export control activities.

1 All Trustees must become members of the company's governing board.

2 The arrangement must provide for the exercise of all prerogatives of ownership by the Trustees with complete freedom to act independently from the foreign owners, except as provided in the agreement, which may limit the authority of the Trustees by requiring approval from the foreign owners with respect to matters such as:

a The sale or disposal of the company's assets or a substantial part thereof;

b Pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;

c Mergers, consolidations, or reorganizations;

d Dissolution of the company; and

e Filing of a bankruptcy petition.

3 The Trustees assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner will be insulated from the company and will solely retain the status of a beneficiary.

4 The company must be organized, structured, and financed to be capable of operating as a viable business entity independent from the foreign owner.

(2) Proxy Agreement. Like the Voting Trust Agreement, under this arrangement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government.

(a) Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders by the irrevocable Proxy Agreement. Legal title to the shares remains with the foreign national(s).

(b) All provisions of a Voting Trust Agreement applicable to Trustees, including authorized limitations on the powers of the Trustees, must apply to the Proxy Holders.

(c) The Proxy Agreement does not impose any restrictions on the organization's eligibility to have access to classified information or matter or to compete for classified contracts.

(d) The company must be organized, structured, and financed to be capable of operating as a viable entity independent from the foreign owner.

(e) Use of a Proxy Agreement requires the establishment of a GSC to oversee classified, SNM/OANM, and export control activities.

(3) Special Security Agreement (SSA). An SSA may be considered when a U.S. organization is effectively owned or controlled by a foreign interest and the Federal Government has entered into a general security agreement with the foreign government involved.

(a) The SSA preserves the foreign shareholder's right to be represented on the governing body with a direct voice in the business and management of the company while denying unauthorized access to classified information or matter, or SNM/OANM by imposing substantial security and export control measures within an institutionalized set of corporate practices and procedures.

(b) An SSA must:

1 Require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens.

2 Provide for the establishment of a GSC to oversee classified, SNM/OANM, and export control activities.

3 Be based on a Secretarial Waiver as described above if the entity is controlled by a foreign government and the contract will require access to proscribed information.

Require an NID prior to release of proscribed information to the contractor or its cleared employees to certify that release of such information is consistent with the national security interests of the United States; provided, however, that in accordance with Section 842 of

Public Law 115- 232, covered NTIB entities (as defined at Section 842(c)(1) of Public Law 115-232) are not required to obtain a NID as a condition for access to proscribed information.
The NID can be program, project, or contract specific.

e. Non-controlling Foreign Ownership. A non-controlling foreign ownership is one in which a foreign national(s) owns less than a majority of the voting securities of the U.S. organization and/or is not in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from non-controlling foreign ownership or control, a FOCI mitigation plan must consist of either Board Resolution or SCA methods.

(1) Board Resolution. When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution by the governing board will normally be adequate to mitigate the FOCI concerns.

(a) The resolution must identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all security and export control requirements; and certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the contractor.

(b) Annual certifications must be provided to the DOE cognizant security office acknowledging the continued effectiveness of the resolution.

(c) The company must distribute to members of its governing board and to its KMP copies of such resolutions, and report in its corporate records the completion of this distribution.

(2) Security Control Agreement (SCA). When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless entitled to representation on the company's governing board, a SCA may be used. There are no access limitations under this type of agreement. However, the SCA requires the imposition of substantial security and export control measures in order to preserve the foreign interest's right to be represented on the board while denying unauthorized access to classified information or matter, or SNM/OANM. The SCA requires the same active involvement in security matters of senior management and certain Board members, and the establishment of a GSC, as are required when the SSA is used.

Limited FCL. A limited FCL may be granted to certain contractors (e.g., a sole source contractor) which are controlled or owned by a foreign interest where

FOCI mitigation is not able to be implemented. Access limitations are inherent with granting limited FCLs. Full requirements for granting a limited FCL are set forth in the Attachment 2 of this Order.

f. Factors Not Related to Foreign Ownership. When factors not related to ownership are present, positive measures must be put in place to assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include:

(1) Modification or termination of loan agreements, contracts and other understandings with foreign interests;

(2) Diversification or reduction of foreign-source income;

(3) Demonstration of financial viability independent of foreign interests;

(4) Elimination or resolution of problem debt;

(5) Assignment of specific oversight duties and responsibilities to board members;

(6) Formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts;

(7) Physical or organizational separation of the contractor component performing on classified contracts;

(8) The appointment of a technology control officer;

(9) Adoption of special Board Resolutions; and

(10) Other actions that negate or mitigate foreign influence.

g. Noncompliance with Mitigation Plans. When the DOE cognizant security office determines that a cleared contractor or its tier parent is out of compliance with an approved FOCI mitigation plan, the cognizant security office must analyze the noncompliance and evaluate the overall impact to the protection of security interests. Depending on the severity of the noncompliance issue and the willingness or unwillingness of the organization to correct the problem and return to compliance, one or more of the following actions must be taken and the cognizant contracting officer notified immediately:

(1) Request a corrective action and implementation plan from the contractor to bring it into compliance with the approved mitigation plan.

(2) Suspend the FCL.

Terminate the FCL. An existing FCL must be revoked if security measures

cannot be taken to remove the possibility of unauthorized access or adverse effect on contract performance

ATTACHMENT 4
CLASSIFIED MAIL CHANNELS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

The Classified Mail Channel (CMC) program regulates physical transmission of classified matter between approved Other Government Agency (OGA) or OGA Contractor (OGA-C)] facilities to meet the requirements of 32 CFR 2001, 32 CFR 117, 10 CFR 1045, and/or the current versions of DOE O 452.8, *Control of Nuclear Weapon Data*, and DOE O 471.6, *Information Security*. This program provides the means for verifying the classification and storage capabilities of approved facilities**.**

2. CMC REQUIREMENTS:

a. Transmission and receipt of classified matter must comply with requirements in DOE O 471.6, current version.

b. Receipt and storage of all classified Nuclear Weapons Data, CNWDI, or Sigmas must be processed and approved in accordance with DOE O 452.8, current version.

c. A Statement of Security Assurance is a mechanism to document the CMC information and identifies the safeguarding capabilities of the facilities.

(1) The Designated Responsible Office (DRO) or appropriate Program Office is responsible to submit and ensure the information within the Statement of Security Assurance is updated periodically.

(2) Statements of Security Assurance that request CNWDI or Sigmas are valid in accordance with DOE O 452.8, current version.

(3) CMCs that are possessing or non-possessing that do not include CNWDI or Sigmas are valid for three years or as identified by the program office (whichever is less).

(4) Revisions, transfers, suspensions, or terminations of SSIMS registrations will be facilitated by the DRO. CMCs that include CNWDI or Sigmas the action must be processed and approved in accordance with DOE O 452.8, current version.

(5) A Statement of Security Assurance provides the following information:

(a) An approved classified mailing address.

(b) The highest level and most restrictive category of classified matter or other security asset the facility is authorized to receive and store.

(c) A statement that classified national security information will be afforded protection according to E.O. 13526, *Classified National Security Information*, and all implementing regulations and directives.

(d) A statement that the requirements of 10 CFR Part 1045, *Nuclear Classification and Declassification*, will be met for RD, FRD, and TFNI.

(e) Assurance that the requirements of the *Atomic Energy Act*, including the mandatory access authorization requirements, will be met for access to RD, FRD, and TFNI.

d. State, local, tribal, and other similar governmental authorities do not have authority to self-certify clearance and security capability for handling classified information. These entities must be handled in accordance with E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, and its implementing directives.

3. ESTABLISHMENT OF A CMC FOR AN OGA.

a. A Statement of Security Assurance must be submitted for all OGAs exchanging any physical classified matter or security asset.

b. Approval of a CMC must be based upon a written Statement of Security Assurance from the OGA that DOE security interests are adequately protected.

c. A CMC must be verified through SSIMS. If not in SSIMS, a new facility must be established.

4. ESTABLISHMENT OF A CMC FOR AN OGA-C.

a. Approval of a CMC must be based upon a written Statement of Security Assurance or Defense Counterintelligence and Security Agency (DCSA) National Industrial Security System (NISS) notification from the OGA-C that DOE security interests are adequately protected.

b. Processing of NWD must be in accordance with DOE O 452.8, current version.

c. CMC must be registered in SSIMS and/or DCSA NISS for an OGA-C organization where DOE does not have a contractual interest but must communicate or exchange classified matter.[12]

[12] DCSA NISS may be used to verify OGA-Cs for exchanging classified matter and security interests other than NWD.

ATTACHMENT 5
CONTROL OF CLASSIFIED VISITS

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. OBJECTIVE. Classified information and matter must be protected by ensuring that only persons with the appropriate security clearances, need-to-know, and programmatic authorizations are afforded access during visits where such information is released or exchanged.

2. PURPOSE. Control of classified visits ensures that access to classified information by cleared U.S. citizens or individuals from foreign governments visiting DOE facilities is controlled in accordance with the mission of the Department and is consistent with national laws and regulations and international treaties and agreements.

3. DEFINITIONS. See Attachment 7. Terms commonly used in the DOE S&S Program are defined in the DOE PIR tool located at https://pir.doe.gov/. In addition to these definitions, the following is provided:

   Senior Federal Official: A Federal employee officially designated and assigned by the Officially Designated Federal Security Authority (ODFSA) to approve classified visits involving access to Restricted Data.

4. REQUIREMENTS. ODFSAs, as designated by the Program Secretarial Officer or, for NNSA, the Office of the Administrator through the Office of Defense Nuclear Security, are responsible for ensuring that the following activities are accomplished for the classified visits program at facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to classified visits must be documented in site security plans. The cognizant security office with support of the contractor must:

   a. Ensure that local procedures are established for processing and handling classified visits by cleared individuals.[13]

   b. Ensure that procedures are established for processing and handling classified visits by foreign nationals in accordance with governing international agreements or treaties.

   c. Ensure that appropriate procedural limitations for classified foreign national visits are documented to preclude access to information not related to the visit and the scope of the international treaty or agreements.

   d. Ensure that responsibility for operational approval of classified visits, including

[13] See DOE O 472.2, *Personnel Security*, current version, for personnel security clearance requirements.

delegations of authority as necessary, is established in writing and documented in the appropriate security plan. The approver must determine that the visit is necessary, and the purpose of the visit cannot be achieved without access to, or disclosure of, classified information.

e. Ensure that, when continuing visitor access approval is necessary for individuals from other government agencies, who frequently visit DOE facilities, the access approval does not exceed a period of 1 year (or for contractors, the final day of a contract if less than one year) and that approval is renewed annually if necessary.

f. Ensure procedures establish that classified visit requests are sent and received through a DOE classified visit processing office and the appropriate security offices of other Federal government agencies.

g. Classified visits involving access to RD by cleared U.S. citizens other than representatives from DOE, DoD, NASA, and NRC must ensure:

(1) An authorized senior Federal official at the site verifies through DOE and national-level personnel security electronic databases the individual's possession of a security clearance at the requisite level.

(2) The authorized Senior Federal Official and makes an affirmative, documented determination that such access will not endanger the common defense and security.

(3) Individuals are given an appropriate briefing concerning the protection of RD prior to being given access;

(4) Individuals sign an acknowledgement that they have received this briefing.

h. Ensure procedures establish that access granted for classified visits is tracked and maintained as part of the site classified visits file and is not entered into any clearance tracking database or extended for any purpose outside the approved classified visit.

i. Ensure procedures establish that all classified information or matter, including the individual's personal notes, to be removed from DOE's control by individuals granted access under paragraph g. above is subjected to a classification review and if classified, is sent through the DOE cognizant security office to the established classified mailing address listed in SSIMS for the OGA or OGA contractor facility which the individual represents. If no classified mailing address is registered in SSIMS, one must be established in accordance with the requirements in Attachment 4 of this Order, before the material is released. Visitors must not hand-carry classified information or matter from DOE premises.

5. VISITS TO DOE FACILITIES BY CLEARED U.S. CITIZENS OTHER THAN DOE PERSONNEL.

a. a. For all classified visits to DOE and DOE contractor facilities, the following must be established and verified by the receiving location:

(1) The identity of the visitor;

(2) The level and type of clearance held by the visitor, which must allow access to the information to be disclosed; and

(3) That the visit is for an official purpose for which the individual has a legitimate need to know and to access the classified information or matter to be disclosed.

b. Appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) must be in place to ensure that the visitor has access only to information for which the individual has a verified need, and that access to other classified information or matter is precluded.

c. Requests for visits and access to specific types of facilities and information must be referred to and approved by the appropriate office:

(1) For weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, the Deputy Administrator for Defense Programs.

(2) For uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy.

(3) For Naval Nuclear Propulsion facilities, the Deputy Administrator for Naval Reactors.

d. Visits involving access to RD when the visitor does not hold a DOE access authorization must be approved by the designated Senior Federal Official. Approval must be based upon verification through DOE and national- level personnel security electronic databases that the individual holds an appropriate final security clearance, unless the individual is in one of the categories described below.

(1) (1) DOE accepts the Q and L access authorizations granted by the NRC as valid for access to RD. Visits by NRC employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology or entry into a DOE classified weapon or production facility must be approved by the appropriate Departmental element office. Visits must be requested

using NRC Form 277, current form. NRC identification badges cannot be used as authority for visits.

(2) (2) Access to RD must be requested on a DOE F 5631.20 (current form), or an OGA's official form, letter, memorandum, or system.

(a) A memorandum or electronic message signed by the certifying official may be used unless access to Nuclear Weapon Data is required. For NASA, the visit request must include a certification that the matter to which access is requested relates to aeronautical and space activities.

(b) Requests must be forwarded for approval to the appropriate Departmental element with jurisdiction over the information to which access is requested. Access to critical nuclear weapon design information must be specifically requested.

(3) Prior to being given access, OGA employees and their contractors who are granted access to RD and SNM in connection with a classified visit must receive an appropriate briefing concerning the protection of RD and SNM and must sign an acknowledgement (e.g., DOE F 5631.18 *Security Acknowledgement* or other approved forms.) indicating their understanding that access will be terminated at the end of the visit period.

(4) RD and/or SNM access granted in connection with a classified visit must be tracked as part of the local site classified visit tracking process, and records of such access must be maintained in the classified visit files. This type of access will not be identified as a Q or L access authorization, will not be entered in the DOE Central Personnel Clearance Index (CPCI) or other clearance tracking databases, and cannot be extended for any purpose outside the approved classified visit.

(5) This process does not apply to classified visits by foreign nationals.

e. Consult DOE O 452.8, *Control of Nuclear Weapon Data,* current version, for additional requirements concerning when access to NWD Sigma information is required.

6. VISITS BY CLEARED DOE PERSONNEL TO OTHER DOE FACILITIES.

a. Unless local site procedures require, or access to certain facilities or programs as described below will take place, formal visit requests are not required for visits by DOE Federal and contractor personnel to other DOE sites. The DOE security badge (e.g., HSPD-12 PIV) will serve as evidence of DOE security clearance/access authorization for internal DOE visits.

b. Visitors who require access to nuclear weapon data (classified Secret or Top Secret), sensitive nuclear materials production information, inertial confinement

fusion data, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by a Departmental element, must obtain approval from the responsible office prior to the visit.

c. DOE F 5631.20 must be used by DOE Federal and contractor employees to obtain programmatic approval for access to Sigmas 14, 15, and/or 20. Approval for access must be obtained from the Deputy Administrator for Defense Programs.

d. Cleared DOE Federal or contractor employees who are foreign nationals may visit other facilities only under the access restrictions which apply to their clearances.

7. CLASSIFIED VISITS TO DOE FACILITIES BY FOREIGN NATIONALS.

a. Ensure that for all classified visits by foreign nationals to DOE facilities, the following must be established and verified:

(1) The identity of the visitor;

(2) Assurance that existing treaty or international agreement covers sharing of specific classified information with the foreign national;

(3) Receipt of security assurances from the appropriate foreign embassy or the visitor's government agency; and

(4) Verification that the appropriate DOE Federal official has approved the sharing of the specific information to be disclosed during the classified visit.

b. DOE Federal or contractor employees may be designated to serve as hosts for classified visits by foreign nationals. A host must be a U.S. citizen with an access authorization equal to or higher than the overall classification of the visit. The host must ensure that:

(1) Foreign nationals are not granted access to classified information before approval is received from the appropriate designated authority with programmatic responsibility.

(2) Foreign nationals are precluded from any access to classified information outside the scope of the international agreement or treaty governing the visit and/or any limitations set by the approval authority with programmatic responsibility, and sharing of classified information is in accordance with the protocols specifically outlined in the agreement or treaty governing the visit (e.g., level, category, and type of classified information, protection procedures for incoming classified foreign government information, security clearance verification, transmission protocols for classified information during and after the visit, post-visit documentation, etc.).

(3) Appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) are in place to ensure that the foreign visitor has access only to information permitted by the applicable international agreement or treaty for which the individual has a verified need, and that access to all other classified information or matter is precluded.

c. Requests for visits and access by foreign nationals to specific types of facilities and information must be referred to and approved by the appropriate Headquarters office:

(1) For visits to uranium enrichment plants or facilities and access to classified information on uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy.

(2) For visits and access to classified information in connection with nonproliferation, international security, or International Atomic Energy Agency requirements, the Deputy Administrator for Defense Nuclear Nonproliferation.

(3) For visits and access to classified information in connection with naval nuclear propulsion, the Deputy Administrator for Naval Reactors.

(4) For visits and access to classified information in connection with Sensitive Compartmented Information, the Office of Intelligence and Counterintelligence.

8. DOCUMENTATION. Reports of classified visits must be maintained in accordance with DOE Administrative Records Schedule 18, paragraph 17.1.

ATTACHMENT 6
INCIDENTS OF SECURITY CONCERN

This Attachment provides information and/or requirements associated with DOE O 470.1A and information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. OBJECTIVE. To ensure the occurrence of an event with detrimental impacts on National Security or Departmental security assets prompts the appropriate graded response, to include an assessment of the potential impacts, appropriate notification, extent of condition, and corrective actions to prevent recurrence. The long-term management of Incidents of Security Concern (IOSCs) serves as an effective Program Planning and Management (PPM) tool for enhancing the specific implementation of security policies (e.g., site-specific implementation).

2. PURPOSE. To set forth requirements for the U.S. Department of Energy (DOE) IOSCs process, including timely identification, notification, inquiry, reporting, and closure of IOSCs. The IOSC program serves multiple purposes to include:

    a. Ensuring IOSCs are communicated to DOE/National Nuclear Security Administration (NNSA) management, U.S. Congress, other agencies, or foreign governments, as appropriate;

    b. Meeting regulatory reporting requirements;

    c. Ensuring IOSCs are assessed relative to the impact to national security and the collateral impact with other programs and security assets;

    d. Enhancing the ability to track and trend the health of DOE federal and contractor security programs;

    e. Enabling mechanisms to support performance assurance, self-assessment, oversight, security awareness, and other key security functions by providing relevant IOSC data; and

    f. Enhancing the ability to influence safeguards and security (S&S) policy development and implementation.

3. DEFINITIONS. See Attachment 7. Terms commonly used in the DOE S&S Program are defined in the DOE PIR tool located at https://pir.doe.gov/. In addition to these definitions, the following are provided:

    a. Administrative Action. In the context of IOSCs, an administrative action refers to any decision (or final proposal) by the organization with official cognizance of an employee to take an adverse or disciplinary action against an employee as a result of an IOSC. This includes formal disciplinary actions taken to correct misconduct and enforce prescribed rules for behavior (e.g., requirements) such as reprimands and suspensions as well as removals, reassignments, furloughs, reductions in

pay/grade, or loss of clearance. Also includes other actions without disciplinary consequences to formally document responsibility and culpability for an IOSC such as formally documented infractions or violations (e.g., using DOE F 5639.3, *Report of Security Incident/Infraction*, or equivalent).

b. Authorized Person. A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

c. Compromise. A final determination that classified information is or was disclosed to one or more unauthorized individuals, or the information was outside of appropriate controls and cannot subsequently be placed back under appropriate controls (e.g., published by media, Unclassified Controlled Nuclear Information (UCNI) or classified information was provided to unauthorized individuals). For the purposes of this Attachment, "compromise" includes an unauthorized dissemination of UCNI (i.e., UCNI is intentionally or negligently transferred to an unauthorized individual). Compromises of classified information are reported as Category A SI IOSCs. Compromises of UCNI are reported as Category B SI IOSCs.

d. Compromise Did Not Occur. A final determination that there is no possibility of compromise. Noncompliances involving classified information where compromise did not occur are typically reported as Category B PI IOSCs.

e. Controlled Unclassified Information (CUI). CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

f. Disposition. Refers to the final determination of a preliminary inquiry whether a potential IOSC (PIOSC) is reportable as an IOSC or does not meet IOSC reporting requirements (i.e., non-IOSC).

g. Diversion (of nuclear material). The diversion of nuclear material refers to the unauthorized removal of nuclear material from its approved or authorized location.

h. Gross Negligence. An action or inaction contrary to requirements or procedures which demonstrates such inattention and carelessness as to appear reckless or intentional. A reasonable person would recognize that the act (or omission) has a high probability of resulting in the loss or compromise of DOE security assets. For example, a person circumvents prescribed procedures with full knowledge of the security requirements and associated penalties but does so for personal

convenience with little concern for the compromise or potential compromise of the security asset. Gross negligence also includes acts (or omissions) which are not deliberate in nature but reflect a recent or recurring pattern of questionable judgement, irresponsibility, negligence, or carelessness. Results in the issuance of a security violation for the responsible individual(s).

(1) Example 1: an individual performing work in a classified subject area is specifically advised that information they are collecting from the open literature is likely classified but does not seek or obtain a Derivative Classifier (DC) review prior to incorporating the information into a document that they generate and then distribute (via unclassified systems or methods).

(2) Example 2: an individual enters a secure area while unconsciously holding a controlled article in their hand and sets it next to a classified computer terminal. Although the individual did not consciously realize they were carrying the controlled article (i.e., did not intend to violate requirements), the oversight demonstrates such inattention and carelessness as to pose a significant risk to sensitive information.

(3) Example 3: an individual needs to photograph an unclassified item in a secure area for a sponsor and, instead of using a properly approved camera, uses their own personal camera because it is more convenient/accessible than the approved camera in a separate building.

i. Inadvertent. An action or inaction contrary to requirements or procedures where neither the act (or omission) nor the outcome were deliberate or intended. Generally, the result of temporary (vs. habitual) inattention while the individual is making a good faith effort to follow prescribed procedures as they understand them.

(1) Example 1: an individual includes information from the open literature (i.e., "open source") in a document (on an unclassified system) without realizing the information is classified. However, in accordance with DOE requirements or local procedures, the individual still appropriately seeks and obtains a DC review prior to distributing the information, during which the issue is identified. (As opposed to "Negligence" Example 1 where the individual made no effort to follow procedure by obtaining a DC review.)

(2) Example 2: an individual may unknowingly bring a controlled or prohibited article into a secure area because they did not perform an adequate check of themselves and the items they were bringing into the area. (As opposed to "Negligence" Example 2 where the individual made no effort to follow procedure by performing a check of themselves.)

(3) Example 3: an individual is instructed to photograph an unclassified item in a secure area for a sponsor using a specific camera but does not realize

the camera's approval for use in the secure area had expired.

j. Incident of Security Concern (IOSC). An action (or inaction) contrary to S&S requirements and which meets DOE reporting requirements because it poses a threat to national security or DOE security assets (i.e., property, personnel, information, capabilities). IOSCs are categorized based on significance, e.g., Category A (more significant) or Category B (less significant) and type. The IOSC type is based on whether compromise or loss occurred; Security Interest (SI), loss or compromise occurred or is suspected, Procedural Interest (PI), a procedural noncompliance that did not result in loss or compromise, or Management Interest (MI), an IOSC reported primarily for management awareness. In addition to regulatory reporting requirements, Procedural Interest and Security Interest IOSCs require a formal inquiry to mitigate the effects and determine the nature, cause, impact, extent, and corrective actions to prevent recurrence.

k. IOSC Category. A designation of an IOSC's significance (e.g., severity):

(1) Category A IOSC. Those IOSCs which have a significant detrimental impact on DOE or national security, often because of the loss, theft, compromise, or potential compromise of a significant security asset (e.g., classified matter, special nuclear material [SNM]). As such, they require the notification and involvement of the Officially Designated Federal Security Authority (ODFSA) and Officially Designated Security Authority (ODSA) (where applicable). Category A IOSCs must also be reported and documented in the Safeguards and Security Information Management System (SSIMS). Category A IOSCs also require a higher level of effort and detail (i.e., graded response) to significantly reduce the likelihood of recurrence (e.g., cause analysis, corrective action plan, extent of condition).

(2) Category B IOSC. Those IOSCs which have a less significant detrimental impact on DOE or national security. These IOSCs typically do not involve the loss, theft, compromise, or potential compromise of significant security assets, but if uncorrected they reasonably could. Category B IOSCs may involve the loss, theft, compromise, or potential compromise of less significant security assets (e.g., UCNI, Unclassified-Naval Nuclear Propulsion Information (U-NNPI). Oversight responsibilities for Category B IOSCs remain with the ODFSA; however, Category B IOSCs are managed and resolved by the ODSA (or equivalent ODFSA designee). Category B IOSCs must be reported either in SSIMS or in a local tracking system as specified in the IOSC Program Plan. When reporting a Category B IOSC, the lower significance must be justified (i.e., loss, theft, compromise, or potential compromise did not occur or is remote). In addition, a lower graded response is typically appropriate.

l. IOSC Type. A subcategorization of IOSCs to indicate the nature of the IOSC;

namely, whether it involves the loss, theft, or compromise of an asset, a procedural violation, or is provided for management awareness.

(1) Security Interest (SI). This type of IOSC involves the loss, theft, compromise, or potential compromise of DOE security assets; this includes, but is not limited to, nuclear weapons and technologies, SNM, classified matter, unauthorized disseminations of UCNI, misuse of U-NNPI, buildings, facilities, government property, employees, and other assets as determined by the ODFSA. The loss, theft, or compromise of significant security assets is typically reported as a Category A IOSC (with the exception of UCNI and U-NNPI).

(2) Procedural Interest (PI). This type of IOSC is associated with the failure to adhere to security procedures and all evidence surrounding the IOSC suggests DOE security assets were not compromised or the likelihood of compromise was remote; however, if uncorrected, the procedural failure could reasonably result in the loss, theft, or compromise of the security asset. Because PI IOSCs are not the result of loss, theft, or compromise, they are typically reported as Category B IOSCs. While not all procedural failures must be reported as PI IOSCs, those procedural noncompliances specified in this Attachment and the IOSC Program Plan must be reported as such.

(3) Management Interest (MI). This type of IOSC is typically the result of external factors outside the direct control of the reporting entity or may only indirectly involve or affect DOE security assets. MI IOSCs may nonetheless have potential undesirable impacts that warrant management and/or oversight notification. The reporting emphasis for MI IOSCs is on notification; therefore, MI IOSCs do not require a formal inquiry, closure report, cause analysis, or corrective actions. Reportable MI IOSCs must be specified in the IOSC Program Plan and categorized as A or B.

m. Lawful Government Purpose (LGP). Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

n. Likelihood of Compromise Is Remote. An inquiry may determine that the likelihood of compromise is remote. For this (final) determination, although protection and control measures are violated, the circumstances associated with the IOSC indicate that there is a low possibility that information was disclosed to unauthorized personnel. Noncompliances involving classified information where the likelihood of compromised is determined to be remote are typically reported as Category B PI IOSCs. Examples include, but are not limited to:

(1) Classified information is left unsecured and unattended for a limited amount of time in an area accessed only by appropriately cleared individuals.

(2) Classified information is discovered on an unauthorized government-furnished computer system or network, but metadata confirms it was only accessed by appropriately cleared individuals.

(3) Unmarked encrypted classified information is transmitted to only cleared recipients on a government-furnished computer system/network not approved for classified information.

o. Mishandle (information). Refers to any action (or omission) contrary to requirements for the protection of that information (e.g., improper storage, improper processing, improper transmission, improper protection).

p. Misuse (of CUI). For the purposes of this Attachment, "misuse of CUI" occurs when someone uses CUI in a manner not in accordance with the policy contained in DOE O 471.7, current version, or the applicable laws, regulations, and government-wide policies that govern the affected information. Except for UCNI and U-NNPI, misuse (including loss) of CUI must be referred to the CUI Designated Element CUI Official (DECO) for handling and reporting in accordance with DOE O 471.7 requirements and do not meet IOSC reporting requirements.

See also Unauthorized Dissemination (of UCNI).

q. Naval Nuclear Propulsion Information (NNPI). Information, classified or unclassified [also known as "U-NNPI"], concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of Naval nuclear-powered ships and prototypes including the associated nuclear support facilities. Also see "U-NNPI" definition.

r. Negligence. An action, inaction, or omission, contrary to requirements or procedures (i.e., noncompliance) that fails to display a reasonable degree of care and attention under the circumstances. The noncompliance could reasonably be expected to result in the loss or compromise of DOE security assets. The noncompliance may be the result of a knowing circumvention of requirements or procedures, but with a good faith expectation of an overriding positive outcome. If loss or compromise of classified information or unauthorized dissemination of UCNI does occur, results in a security violation. If loss or compromise does not occur or if U-NNPI is "misused", typically results in a security infraction for the responsible individual(s). Note: a noncompliance may be unintentional (the responsible individual did not intend the noncompliant outcome) yet still negligent because the individual did not make a good faith effort to follow prescribed procedures.

(1) Example 1: an individual performing work in a classified subject area includes information from the open literature in a document they generate (on an unclassified system) without realizing the information is classified. The individual then distributes the document without obtaining DC

reviews required by DOE or local procedures. (As opposed to "Inadvertent" Example 1 where the individual made a good faith effort to follow procedures prior to dissemination.)

(2) Example 2: an individual unknowingly brings a controlled or prohibited article into a secure area because they did not perform a check of themselves or the items they were bringing into the area (e.g., in a rush, forgot, distracted). (As opposed to "Inadvertent" Example 2 where the individual made a good faith effort to follow procedures by performing a check, albeit an incomplete check.)

(3) Example 3: an individual needs to photograph an unclassified item in a secure area for a sponsor and brings a camera into the area without the appropriate approvals. Although the individual may be aware of requirements, they have a good faith expectation of an overriding positive outcome (i.e., satisfying the sponsor).

s. Non-IOSC. An event (e.g., PIOSC) that did not meet IOSC reporting requirements. Includes noncompliances which do not meet IOSC reporting thresholds as defined in this Attachment or in the IOSC Program Plan.

t. Potential Compromise. At the conclusion of an inquiry into a suspected compromise, there may be inadequate evidence to determine whether a (actual) compromise occurred, did not occur, or whether the likelihood of compromise is remote. In this case, the inquiry will make the final determination that a potential compromise occurred. Although there is no clear indication or evidence of compromise (e.g., no direct recipient), the circumstances associated with the IOSC indicate that there is an obvious possibility that unauthorized disclosure occurred, and compromise is not remote. The IOSC will be treated as a compromise even though there is no definitive evidence that a compromise occurred. (A final determination that a potential compromise of classified matter occurred must be reported as a Category A IOSC.)

u. Potential IOSC (PIOSC). A security-related event or unwanted condition that is or may be contrary to S&S requirements or procedures. PIOSCs may pose a threat to national security or organizational security assets (e.g., property, personnel, information, capabilities) and require a preliminary inquiry to determine if the event meets DOE reporting requirements as an IOSC.

v. Security Asset. For the purposes of this Attachment, an asset or other interest in a S&S topical area (e.g., Information Security, Physical Protection) where a regulatory protection obligation exists. Includes, but is not limited to, nuclear weapons and technologies, SNM, classified matter, UCNI, CUI, buildings, facilities, and government property, and employees. Generally, includes all Protection Level (PL) assets (i.e., PL-1-8). (Note: As defined here, security "assets" are synonymous with security "interests" but are distinguished to avoid confusion with the "Security Interest" IOSC type.)

w. Security Infraction. Security infractions are documented and reported to the Cognizant Personnel Security Office (CPSO) using DOE F 5639.3 or equivalent as documented in the IOSC Program Plan. Infractions are both a method for characterizing a noncompliance that did not result in a (security) violation (i.e., loss, theft, compromise or potential compromise did not occur), as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:

(1) Classified information was mishandled; or

(2) UCNI was handled contrary to Physical Protection Requirements specified in 10 CFR 1017 Subpart E (e.g., failure to: notify of UCNI protection requirements, maintain physical control while in use, store in a manner to preclude unauthorized access, or destroy using authorized means); or

(3) "Misuse" of U-NNPI.

Note: The issuance of a security infraction will only be associated with Category B IOSCs, versus security violations which are issued for Category A IOSCs or Category B IOSCs involving unauthorized disseminations of UCNI.

x. Security Violation. Security violations are documented and reported to the CPSO using DOE F 5639.3 or equivalent as documented in the IOSC Program Plan. Security violations are both a method for characterizing a noncompliance (e.g., a violation of policies or requirements) as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:

(1) The IOSC resulted in the loss, theft, compromise or potential compromise of classified information or unauthorized dissemination of UCNI; or

(2) The IOSC did not result in the loss, theft, compromise or potential compromise but reasonably could be expected to and is the result of gross negligence or a willful act; or

(3) Any knowing, willful, or grossly negligent action to classify or continue the classification of information contrary to federal requirements; or

(4) Any knowing, willful, or negligent action to create or continue a special access program contrary to federal requirements; or

(5) The IOSC is reported as a Category A SI and one or more responsible persons are identified.

y. Significant Atomic Energy Defense Intelligence Losses. Defined by 50 U.S.C. Section 2656 as "any national security or counterintelligence failure or compromise of classified information at a facility of the Department of Energy or

operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interests of the United States."

z. Site. One or more entities (e.g., facilities, programs, organizations) operating under a centralized security management, with consolidated authority and responsibility for the security operations and typically covered by a site security plan. As used in this Attachment, refers to federally operated or contractor-managed locations, offices, departments, or programs.

aa. Suspected Compromise. Information is provided which indicates a compromise may have occurred, but no clear confirmation exists. A local inquiry reviews the circumstances to determine whether a potential compromise or (actual) compromise occurred. A suspected compromise is not a final determination of compromise status.

bb. Unauthorized Dissemination. The intentional or negligent transfer of UCNI to any person other than an Authorized Individual (i.e., a person who has routine access to UCNI under 10 CFR 1017.20) or a person granted limited access to UCNI under 10 CFR 1017.21.

cc. Unclassified Controlled Nuclear Information (UCNI). Certain unclassified Government information concerning nuclear facilities, materials, weapons, and components whose dissemination is controlled under section 148 of the Atomic Energy Act and 10 CFR 1017.

dd. Unclassified Naval Nuclear Propulsion Information (U-NNPI). Unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. Also see "NNPI" definition.

ee. Willful. A willful noncompliance refers to a determination that an employee deliberately disregarded (i.e., ignored), intentionally violated, or was aware of a violation of, a security requirement and, in addition, the employee either attempted to conceal the violation or made no reasonable attempt to eliminate or abate the conditions that gave rise to the violation. Willful noncompliances must be reported through SSIMS. Results in the issuance of a security violation for the responsible individual(s).

(1) Example 1: an individual collecting information in a classified subject area where DOE requirements or local procedures dictate a DC review but does not appropriately seek or obtain a DC review prior to distributing the information and, after an IOSC is reported, falsifies records to indicate DC reviews had been obtained.

(2) Example 2: an individual performing work in a classified subject area is

specifically advised that the information is classified but distributes the information using unauthorized means or to unauthorized personnel, nonetheless.

(3) Example 3: an individual knows a coworker used their personal phone to take a picture of a properly marked classified document for later reference from home to perform work remotely. Both the individual who knows about the violation (and made no attempt to report or halt it) and the coworker who took the initial improper action are responsible for willful violations.

4. REFERENCES.

a. 18 U.S.C. Section 923 (g)(6), *Licensing*. Each licensee shall report the theft or loss of a firearm from the licensee's inventory or collection, within 48 hours after the theft or loss is discovered, to the Attorney General and to the appropriate local authorities.

b. 42 U.S.C. Sections 2271 to 2181, *Enforcement of Chapter,* gives the U.S. Federal Bureau of Investigation (FBI) the authority to investigate alleged or suspected criminal violations of the Atomic Energy Act, makes violations of the Act criminal, and provides for injunction and contempt proceedings.

c. 42 U.S.C. Section 2282b (Section 234B, as amended), establishes civil penalties for violations of directives regarding protection of classified information by contractors or their employees.

d. 42 U.S.C. Section 5801, 5877 and 307, *Energy Reorganization Act of 1974,* requires investigating suspected, attempted, or actual thefts of SNM in the licensed sector and developing contingency plans for dealing with such events.

e. 50 U.S.C. Section 402a, *Coordination of Counterintelligence Activities,* states that the FBI is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

f. 50 U.S.C. Section 2656, *Notice to congressional committees of certain security and counterintelligence failures within nuclear energy defense programs*, requires the Secretary of Energy to notify the Committees for Armed Services of the U.S. Senate and House of Representatives of each "significant atomic energy defense intelligence loss."

g. E.O. 13526, *Classified National Security Information*. If the Director of the Information Security Oversight Office finds that a violation of this policy or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

h. National Security Decision Directive 84, *Safeguarding National Security Information*, requires unauthorized disclosures of classified information to be evaluated to determine information disclosed and extent of dissemination, and discusses coordination with the U.S. Department of Justice.

i. National Security Presidential Memorandum-32 (NSPM-32), *Establishing a Standardized Procedure for Reporting Presidential Critical Information Requirements*, requires consistent, standardized reporting to the Executive office of the President pertaining to national-level incidents and crises.

j. 6 CFR Part 27, *Chemical Facility Anti-Terrorism Standards,* establishes the standards for possessing or planning to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department.

k. 7 CFR Part 331, *Possession, Use, and Transfer of Select Agents and Toxins*, implements the provisions of the *Agricultural Bioterrorism Protection Act of 2002* setting forth the requirements for possession, use, and transfer of select agents and toxins. The biological agents and toxins listed in this part have the potential to pose a severe threat to plant health or plant products.

l. 9 CFR Part 122, *Organisms and Vectors*, establishes the permits required, the application for permits and the suspension or revocation of the permits.

m. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, establishes rules to assess a penalty for violation of a directive relating to the protection of classified information pursuant to 42 U.S.C. Section 2282b (Section 234B, as amended, of the Atomic Energy Act) or for violation of a compliance directive that directs action for the protection of classified information.

n. 10 CFR Part 1016, *Safeguarding of Restricted Data by Access Permittees,* requires the permittee to report any infractions, losses, compromises, or possible compromise of Restricted Data.

o. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information,* implements section 148 of the Atomic Energy Act which prohibits the unauthorized dissemination of UCNI, establishes minimum physical protection standards for UCNI, and established a procedure for the imposition of penalties on persons who violate section 148 of the Atomic Energy Act or 10 CFR part 1017.

p. 10 CFR Part 1045.25, *Nuclear Classification and Declassification,* addresses the sanctions for knowing, willful, or negligent actions contrary to the requirements of the CFR that results in the misclassification of information.

q. 32 CFR 117, *National Industrial Security Program Operating Manual (NISPOM)*, Subpart 117.8, "Reporting Requirements," requires any reports of

loss, compromise, or suspected compromise of classified information, foreign or domestic, to be reported to the cognizant security agency (CSA). Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise. Requires the final report to document culpability and disciplinary actions.

r. 32 CFR Part 2001, *Classified National Security Information*. Part 2001.48, "Loss, Possible Compromise or Unauthorized Disclosure", mandates reporting, inquiry, etc., for the loss, possible compromise, or unauthorized disclosure of classified information. If the event entails a criminal violation, coordination is required with legal counsel and the Department of Justice.

s. 32 CFR Part 2002, *Controlled Unclassified Information* (CUI), describes the executive branch's CUI Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI. Includes definitions for misuse of CUI and reporting requirements.

t. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*. Supplements 48 CFR Chapter 1, *Federal Acquisition Regulation* (FAR), and includes the security provisions and clauses to be used in DOE solicitations and contracts when a facility clearance and/or access to classified information will be necessary for the performance of the contract. Includes the security clauses to be used in DOE solicitations and contracts or agreements involving access to classified information and/or a significant quantity of special nuclear material (SNM).

u. DOE O 151.1, *Comprehensive Emergency Management System*, current version, establishes policy and assigns roles and responsibilities for the DOE Emergency Management System.

v. DOE O 205.1, *Department of Energy Cybersecurity Program*, current version, enables accomplishment of DOE mission to fulfill Federal cybersecurity requirements and protect DOE information systems. Establishes policy for incident response and reporting requirements for events impacting DOE information systems.

w. DOE O 206.1, *Department of Energy Privacy Program*, current version, establishes Departmental implementation of agency statutory and regulatory requirements for privacy, specifically those provided in the *Privacy Act of 1974*, as amended, and Office of Management and Budget directives.

x. DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of Inspector General* [IG], current version, establishes requirements and responsibilities for reporting fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement to the DOE, IG.

y. DOE O 231.1, *Environment, Safety, and Health Reporting*, current version, requires a timely collection, reporting, analysis, and dissemination of information on environment, safety, and health issues as required by law or regulations or as

needed to ensure that DOE and NNSA are kept fully informed on a timely basis about events that could adversely affect the health and safety of the public or the workers, the environment, the intended purpose of DOE facilities, or the credibility of the Department.

z. DOE O 232.2, *Occurrence Reporting and Processing of Operations Information*, current version, ensures that DOE and NNSA are informed about events that could adversely affect the health and safety of the public or the workers, the environment, DOE missions, or the credibility of the Department; and establishes requirements for occurrence reporting and notification and reporting processes.

aa. DOE O 333.1, *Administering Work Force Discipline, Adverse and Performance Based Actions*, current version, provides DOE requirements and responsibilities for administering work force discipline and corrective actions. (Does not apply to contractors.)

bb. DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, current version, establishes the policy, process and procedures for control of sensitive use control information in nuclear weapon data (NWD) categories Sigma 14 and Sigma 15 to ensure that dissemination of the information must be restricted to individuals with valid need to know as well as IOSC reporting requirements.

cc. DOE O 457.1, *Nuclear Counterterrorism*, current version. Defines requirements for the protection of sensitive improvised nuclear device information and provides a framework to support DOE activities related to nuclear counterterrorism.

dd. DOE O 470.3, *Design Basis Threat (DBT),* current version, defines DOE's physical protection strategies as well as National Security Assets and their associated protection levels (PLs).

ee. DOE O 470.4, *Safeguards and Security Planning*, current version, establishes Departmental Safeguards and Security Planning requirements and responsibilities.

ff. DOE Order 471.1, *Identification and Protection of Unclassified Controlled Nuclear Information* [UCNI], current version. Provides requirements and responsibilities for identifying and protecting against the unauthorized dissemination of UCNI.

gg. DOE O 471.7, *Controlled Unclassified Information*, current version, establishes the DOE CUI Program and documents a policy for designating, handling, and reporting the misuse of information that qualifies as CUI.

hh. DOE O 473.1, *Physical Protection Program*, current version, establishes requirements for the Department of Energy (DOE) Physical Protection (PP) Program for assets under the control of DOE. Includes protection requirements for Protection Level (PL) assets.

ii. DOE O 473.2, *Protective Force Operations*, current version, includes protection

and reporting requirements for DOE firearms, explosives, ammunition, or any other pyrotechnic, ammunition, or training devices not legal for civilian sale, as well as descriptions of use of force.

jj. DOE O 474.2, *Nuclear Material Control and Accountability*, current version, establishes requirements for developing, implementing, and maintaining a nuclear material control and accountability (MC&A) program within the U.S. Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), and for DOE-owned materials at other facilities that are exempt from licensing by the Nuclear Regulatory Commission (NRC).

kk. DOE O 475.1, *Counterintelligence Program*, current version, establishes DOE Counterintelligence (CI) Program requirements and responsibilities for the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA). Includes requirements to conduct investigations and inquiries of CI or counterterrorism concerns.

ll. DOE O 475.2, *Identifying Classified Information*, current version, establishes the program to identify and protect information classified under the Atomic Energy Act (i.e., Restricted Data [RD], Formerly Restricted Data [FRD], Transclassified Foreign Nuclear Information [TFNI]) or E.O. 13526, *Classified National Security Information*.

mm. *DOE Enforcement Coordinator Handbook* serves as a reference and source of guidance for DOE and contractor personnel to facilitate performance of regulatory compliance responsibilities. Includes requirements to report willful acts in SSIMS.

nn. National Archives and Records Administration CUI Registry, the online repository for information, guidance, policy, and requirements on handling CUI at the federal level. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. DOE maintains a DOE CUI list of approved CUI categories authorized for DOE use.

5. ROLES AND RESPONSIBILITIES.

a. Officially Designated Federal Security Authority (ODFSA). For the purpose of this Attachment, the ODFSA defines the Federal designee(s) (e.g., program office, individual, and/or site office) responsible for executing the subsequent roles and responsibilities. Note: The term ODFSA refers to either the ODFSA or their official designee(s).

(1) Coordinates formal reviews of IOSCs involving the loss, theft, compromise, or potential compromise of Top Secret, Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Restricted Data (RD) Nuclear Weapon Data to determine whether the

IOSC constitutes a "significant atomic energy defense intelligence loss."

(2) In accordance with 50 U.S.C. 2656, if the IOSC meets the "significant atomic energy defense intelligence loss" criteria, the ODFSA initiates notification to the Secretary of Energy through the Program Secretarial Officer for notification to the Committees on Armed Services of the Senate and House of Representatives, after consultation with the Director, National Intelligence, and the Director, FBI. Notification of a "significant atomic energy defense intelligence loss" must occur no later than 30 days after the IOSC was determined to constitute a "significant atomic energy defense intelligence loss."

(3) In accordance with 32 C.F.R. 2001.48, the ODFSA initiates notification of the Director, Information Security Oversight Office (ISOO), if a violation of the requirements to protect classified information involves any of the following:

(a) Notification to oversight committees in the Legislative branch;

(b) Significant public attention;

(c) Large amounts of classified information;

(d) The revelation of a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(4) In accordance with NSPM-32 requirements, the ODFSA:

(a) Anticipates and assesses those IOSCs which will be of interest to the Secretary of Energy given the events' significance or national-level implications.

(b) Immediately reports IOSCs which will be of interest to the Secretary of Energy to their responsible Emergency Operations Center (EOC).

(c) Seeks guidance and clarification on NSPM-32 reporting requirements and specific potential NSPM-32 reportable events from their responsible EOC or the Office of Emergency Management (e.g., through the Request for Information [RFI] process).

(d) Ensures site-specific thresholds for significant national-level events are addressed in the IOSC Program Plan as well as processes for providing immediate notifications to the ODFSA.

(5) Reviews all Category A IOSCs. Serves as the liaison to Congress, the Secretary, other government agencies, the FBI, and the IG for IOSCs under

their purview. If a compromise involves the classified matter of another Federal agency, the ODFSA coordinates with the other government agencies (CSAs), as appropriate.

(6) Tracks and trends IOSCs for the purpose of assessing program strengths and weaknesses across programmatic offices, departments, and sites.

(7) Approves the IOSC Program Plan in consultation with the cognizant DOE General Counsel.

(8) Ensures that the IOSC Program Plan addresses all elements of the program and that sufficient resources are provided to conduct inquiries and to implement corrective actions.

(9) Performs IOSC program implementation oversight to include, but not limited to, reviewing inquiries, conducting determinations of compromise, tracking and trending, and integrating of the data into the larger PPM function.

(10) Ensures that the ODSA completes the actions necessary to resolve IOSCs, including actions necessary to prevent recurrence.

(11) Utilizes the IOSC program as a feedback mechanism to assist management in evaluating programmatic performance across all security disciplines.

(12) Coordinates with the Deputy Director, Counterintelligence Directorate, concerning IOSCs that indicate a deliberate compromise of classified information or that involve foreign persons, governments, or activities.

b. Office of Environment, Health, Safety and Security (EHSS).

(1) Establishes IOSC policies for the Department based on national policies and best business practices.

(2) Oversees and maintains SSIMS in a manner consistent with the requirements of this Attachment.

(3) Provides SSIMS training.

(4) Assesses IOSC data for the purpose of reviewing and enhancing security policies.

(5) Provides technical IOSC and causal analysis expertise to site and program offices as requested.

c. Office of Enforcement (EA-10). The Office of Security Enforcement (EA-13) enforces provisions under 10 CFR Parts 824 and 1017, which implement subsections a, c, and d of section 234B of the *Atomic Energy Act of 1954*, 42 U.S.C. Section 2282b.

d. Office of Chief Information Officer (CIO).

(1) Performs cyber-incident response and recovery.

(2) Establishes, implements, and disseminates policies, procedures, and capabilities to Contractor and Federal Cybersecurity Programs elements for appropriate cyber-incident response (e.g., the sanitization of information from unauthorized computer systems or networks).

(3) Establishes, implements, and disseminates policies, procedures, and independent reporting requirements (i.e., non-IOSC) for events involving the misuse (including loss) of CUI.

e. Office of Emergency Management. The DOE/NNSA Office of Emergency Management (NA-40) develops and issues the Department Critical Information Requirements, per DOE O 151.1, current version. This includes identifying and reporting Presidential Critical Information Requirements (PCIRs), including those events with an IOSC nexus, to the White House Situation Room (WHSR).

f. Officially Designated Security Authority (ODSA).[14] The ODSA bears primary responsibility for compliance with the IOSC program requirements at facilities or within operations (e.g., site-specific) and ensures the following activities are appropriately assigned and carried out. These responsibilities include, but are not limited to:

(1) Ensures an IOSC Program Plan is developed consistent with the requirements of this Attachment.

(2) Integrates the IOSC Program Plan with the larger PPM function for the purpose of influencing other functions and enhancing the implementation of security policies (e.g., site-specific implementation).

(3) Oversees and assesses all IOSCs to ensure they are categorized in accordance with the requirements of this Attachment.

(a) Ensures IOSCs receive the appropriate levels of notification(s) and coordination.

[14] For the purposes of this Attachment, the term ODSA refers to either the ODSA or the equivalent ODFSA designee(s), where appropriate.

(b) Ensures IOSCs receive the appropriate level of causal analyses, corrective actions, impact assessments, and other mitigating activities.

(4) Ensures that any documents generated concerning IOSCs are reviewed for classification as required by DOE O 475.2, *Identifying Classified Information,* current version, as applicable.

(5) Tracks and trends IOSCs to monitor security program performance and modify site security procedures accordingly.

(6) Assesses the impacts of IOSCs relative to other programs and security assets and coordinates with the programmatic element responsible for the information that is compromised or suspected of compromise.

(7) Utilizes the IOSC program as a feedback mechanism to assist management in evaluating programmatic performance across all security disciplines.

(8) Advises the ODFSA of adverse trends or other indicators that security plans and/or procedures are not achieving the desired results.

(9) Ensures IOSCs caused by sub-contractors are reported consistent with the requirements of this Attachment.

(10) Ensures appropriate resources are allocated to identify the cause(s) of IOSCs and develop and track corrective actions to prevent recurrence.

(11) Ensures that all applicable processes and responsibilities supporting the requirements of this Attachment are documented in the IOSC Program Plan.

ATTACHMENT 6
SECTION 1: INCIDENTS OF SECURITY CONCERN REQUIREMENTS

This Attachment provides information associated with DOE O 470.1A and information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL REQUIREMENTS.

   a. Each IOSC, except for MI IOSCs (see 3c.(2) of this Section), requires categorization, an initial notification report, an inquiry, and a final IOSC inquiry report (i.e., closure report). The level of effort associated with the latter three steps is graded based on the IOSC category and the factors (severity, asset, etc.) surrounding the IOSC (i.e., graded response).

   b. Initial and final reporting is imperative as the ODFSA has specific responsibilities for notifying and/or coordinating with other agencies, governments, Departmental leadership, and Congress for select IOSCs.

   c. All information generated as part of this process must be protected according to its sensitivity and/or classification determination.

   d. IOSCs include a range of possible actions, inactions, or events that:

      (1) Pose threats to national security interests and/or Departmental security assets;

      (2) Create potentially serious or dangerous security situations;

      (3) Have a significant effect on the S&S Program's capability to protect DOE security assets;

      (4) Indicate a failure to adhere to security requirements or procedures as documented in Federal guidance or other applicable local requirements (e.g., IOSC Program Plan); or

      (5) Illustrate a security system is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

   e. IOSCs which involve the loss, theft, compromise, or potential compromise of classified matter (to include classified NNPI) or diversions of SNM must be categorized based on the merits at the time of the original occurrence. Although factors may mitigate an IOSC between occurrence and discovery/reporting (i.e., after the fact), these factors do not impact the appropriate categorization which must be based solely on factors at the original time of occurrence.

2. IOSC PROGRAM PLAN. The IOSC Program Plan is developed by the ODSA (or equivalent ODFSA designee) and approved by the ODFSA. The IOSC Program Plan addresses each component of this Attachment, integrates the IOSC Program Plan with the larger PPM function and includes implementation guidance from the ODFSA describing expected actions or responses for the individual requirements. The IOSC Program Plan must include, but is not limited to, the following elements:

   a. Specific Federal offices and entities requiring IOSC notifications.

   b. ODFSA thresholds for significant national-level events which may require NSPM-32 reporting through the responsible EOC and DOE/NNSA Office of Emergency Management. This includes timeframes and processes for providing immediate notifications to the ODFSA (outside of formal IOSC reporting requirements) when there is confirmation or high confidence in a significant national-level event.

   c. The process for notifying entities within cognizant management; to include entities requiring notification and required content of notification reports.

   d. The process for informing key stakeholders (e.g., Cybersecurity, Occurrence Reporting Processing System [ORPS], ODFSA) of potential "significant" or "national level" security events that require more immediate notifications (i.e., outside IOSC processes described in this Attachment).

   e. The process whereby the IOSC Program is informed of PIOSCs described in this Attachment.

   f. The process for notifying other impacted stakeholders of compromises or suspected compromises (of others' information).

   g. The process for coordinating and identifying the lead IOSC Program for IOSCs which fall under the purview of two or more Program Offices (e.g., impacts more than one site).

   h. How IOSC containment activities are coordinated with applicable stakeholders (e.g., Cybersecurity), carried out, and documented.

   i. Whether Category B IOSCs will be reported in SSIMS or in a local tracking system.

   j. The circumstances and process, if any, for obtaining and approving limited exceptions to reporting timeframes.

   k. The expected timeframe for completing inquiries and seeking extensions.

   l. The process for reporting or closing IOSCs if SSIMS is unavailable.

   m. The process and content for providing IOSC reports (e.g., final IOSC closure

report) to required stakeholders; to include the ODSA, ODFSA (as appropriate), and CPSO.

n. Those events identified by the ODFSA or ODSA that must meet IOSC reporting requirements as an MI IOSC (in addition to those identified in this Attachment). Includes identifying the appropriate IOSC categories.

o. Other security assets identified by the ODFSA or ODSA for which the loss, theft, compromise, or potential compromise must be reported as an SI IOSC (in addition to those security assets identified in this Attachment). In accordance with DOE O 470.3, current version, must include PL-1 through PL-8 assets possessed by the facility/program for which the loss, theft, or compromise must be reported as an IOSC.

p. Other procedural noncompliances identified by the ODFSA or ODSA that must be reported as PI IOSCs (in addition to those identified in this Attachment).

q. How resources are allocated or provided to conduct inquiries, perform cause analysis, implement, and track corrective actions, and validate the effectiveness of corrective actions.

r. Any radiological, chemical, and/or biological materials possessed by the site, which, if misused or unaccounted for, could endanger the public and require IOSC reporting (e.g., PL-1 through PL-7 assets).

s. The process and thresholds for reporting IOSCs involving controlled and prohibited articles.

t. The specific implementation (e.g., site-specific) of the preliminary inquiry, categorization, inquiry, reporting (i.e., initial notification report and final closure report), and IOSC closure processes.

u. The process for providing other impacted stakeholders a "right of first refusal" and when and how inquiry activities will cease and be transferred to others (e.g., CI, FBI, FIE, IG).

v. The specific processes for handling, coordinating, and reporting Special Reporting Situations.

w. The process for training, certifying, and appointing inquiry officials and other designated personnel performing IOSC support activities in a training capacity pending final appointment.

x. The process for documenting and reporting security infractions and violations; whether DOE F 5639.3 is used, or an equivalent, and how they are reported to the CPSO.

y. How information regarding disciplinary and administrative actions is coordinated,

tracked, and reported between applicable stakeholders (e.g., HR, CPSO, HSPD-12 verification office).

3. IOSC IDENTIFICATION AND CATEGORIZATION. DOE uses a graded response for the identification, categorization, and subsequent handling of IOSCs based on the sensitivity of the security asset being protected (and as evidenced through the IOSC category and type). This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and cause analysis of, IOSCs. A graded response allows resources to be effectively allocated to implement the requirements of this Attachment.

a. All IOSCs must be categorized by significance level and type. As Table 1 illustrates, there are two levels of significance and three types of IOSCs.

Table 1. Significance Levels and IOSC Types

SIGNIFICANCE LEVEL CATEGORY	
A	B
IOSC TYPE	
Security Interest (SI)	Security Interest (SI)
Management Interest (MI)	Management Interest (MI)
Procedural Interest (PI)	Procedural Interest (PI)

b. IOSC Significance Level Categories.

(1) Category A IOSCs are those that have a significant detrimental impact on DOE or national security. Often, this impact is the result of a loss, theft, compromise, or potential compromise of a significant security asset (e.g., classified information, sensitive compartmented information facilities, facilities storing, processing, and transmitting classified information and/or matter, SNM, and certain radiological chemical or biological materials). Category A IOSCs require the notification and involvement of the ODFSA and reporting through SSIMS. The involvement of the ODFSA for Category A IOSCs is imperative for assessing impacts, coordinating with external agencies, and/or notifying senior management. Category A IOSCs also require a higher level of effort and detail (i.e., graded response). This includes a cause analysis and corrective action plan for SI and PI IOSCs to significantly reduce the likelihood of recurrence.

(2) Category B IOSCs are those that have a less significant detrimental impact on DOE or national security. Category B IOSCs do not involve the loss, theft, compromise, or potential compromise of a significant security asset;

however, if uncorrected they reasonably could. Category B IOSCs may involve the loss, theft, or compromise of other less significant security assets (e.g., automated data processing centers, vital equipment, Other Accountable Nuclear Material (OANM), certain radiological chemical or biological materials, UCNI, U-NNPI, or other Departmental property). Category B IOSCs are managed and resolved at a lower level than Category A IOSCs (e.g., by the ODSA), under ODFSA oversight, to proactively address reoccurring IOSCs and minimize the occurrence of potentially more significant IOSCs. Although the less significant categorization must be justified (i.e., loss, theft, compromise, or potential compromise of a significant security asset did not occur or is remote), a lower graded response is typically appropriate.

c. IOSC Type. A subcategorization of IOSCs to indicate the nature of the IOSC; namely, whether it involves the loss, theft, or compromise of an asset, a procedural violation, or is provided for management awareness.

(1) Security Interest (SI). This type of IOSC involves the loss, theft, compromise, or potential compromise of DOE security assets; this includes nuclear weapons and technologies, SNM, classified matter, UCNI, U-NNPI, and other PL-1 through PL-8 security assets as specified by the ODFSA in the IOSC Program Plan (e.g., critical program assets, national critical infrastructure, and sabotage targets).

(2) Management Interest (MI). This type of IOSC does not necessarily involve Departmental assets but has other potential undesirable (security) impacts. MI IOSCs differ from SI and PI IOSCs in that the emphasis is on notification; therefore, MI IOSCs do not require a formal inquiry, closure report, cause analysis, or corrective actions, but must be categorized as A or B.

(3) Procedural Interest (PI). This type of IOSC is associated with the failure to adhere to security procedures, and all evidence surrounding the IOSC suggests the security asset was not compromised or the likelihood of compromise was remote. However, if uncorrected the procedural failure could reasonably result in the compromise or potential compromise of the security asset. While not all procedural failures must be reported as PI IOSCs, those procedural noncompliances specified in this Attachment and the IOSC Program Plan must be reported as such.

d. IOSC Criteria. Based on the three types of IOSCs, the following provides a general framework for distinguishing between Category A and B IOSCs.

(1) SI.

(a) Category A SI IOSCs result in the issuance of a security violation to the responsible individual(s) and include, but are not limited to:

1 Loss, theft, diversion, or unauthorized access to (e.g., compromise of) accountable quantities of Category I or II SNM or other nuclear material controlled and accounted for as SNM in accordance with DOE O 474.2, current version. (Note: "Loss" does not include quantities that are within established shipping, processing, and inventory limits);

2 Loss, theft, or diversion of accountable quantities of Category III or IV SNM.

3 Loss, theft, compromise, or potential compromise of classified matter;

4 Unauthorized disclosure of Sigma 14 or 20 Nuclear Weapon Data (NWD) to a Q-cleared person where the Use Control Site Coordinator (UCSC), Use Control Program Coordinator (UCPC), or Site Sigma 20 Coordinator determines the disclosure should be reported as an IOSC (in accordance with DOE O 452.7) and DOE O 457.1, current version;

5 Loss, theft, or unauthorized access to (e.g., compromise of) a quantity of radiological, chemical, and/or biological materials that, if misused, could endanger the public (materials and quantities, if any, which pose such a risk must be specified in the IOSC Program Plan);

6 Loss or theft of security key, keycard, or badge (e.g., DOE PIV) which provides unimpeded access to SNM or classified matter (e.g., direct access versus access impeded by other multi-factor layers/measures);

7 Loss, theft, or other inventory shortages of DOE firearms, explosives, 100 rounds or more of any live-fire ammunition, or any other pyrotechnic, ammunition, or training device not legal for civilian sale, purchase or use (in accordance with reporting requirements in DOE O 473.2, current version);

8 Loss, theft, compromise, or potential compromise of foreign government material or information that requires reporting based on established agreements and required protocols;

9 Loss, theft, compromise, or potential compromise of other assets determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan; or

10 Other assets as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

(b) Category B SI IOSCs typically result in the issuance of a security infraction to the responsible individual(s), with the exception of UCNI, which results in a security violation. Category B SI IOSCs include, but are not limited to:

1 Confirmed theft or diversion with malicious intent (e.g., attempted theft) of OANM (that does not meet the threshold of SNM);

2 Unauthorized disclosure of Sigma 15 Nuclear Weapon Data (NWD) to a Q-cleared person which would not be otherwise approved (i.e., after the fact by the UCSC or the UCPC);

3 Loss, theft, or unauthorized dissemination of UCNI;

4 Intentional or negligent "misuse" of significant CUI- in accordance with DOE O 471.7, current version. "Misuse" reportable as an IOSC includes, but is not limited to:

a Information from a properly marked U-NNPI document or matter is intentionally released to someone who does not have an LGP;

b Intentionally or negligently releasing a U-NNPI - marked document (or matter), in its entirety, to someone who does not have an LGP;

c Any other misuse of CUI will be handled in accordance with DOE O 471.7 by the element assigned programmatic responsibility for the information (e.g., referred to the designated cognizant CUI liaison).

5 Other assets as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

(2) MI.

(a) Category A MI IOSCs are significant enough to warrant notification to the ODFSA. Examples include, but are not limited to:

1 Work stoppages as a result of planned or unplanned events with security impacts;

2 Civil disturbances or disorder causing immediate danger or resulting in damage or injury;

3 Any person or persons acting in a manner perceived to cause immediate harm or violence (e.g., wielding a weapon, active shooter);

4 Credible (e.g., actionable) threats of violence against DOE personnel or facilities which results in emergency response activities (e.g., bomb threat that results in emergency response or other law enforcement response);

5 Deliberate penetration of a security barrier or boundary where classified matter or SNM is stored;

6 Deliberate tampering or circumvention of security barriers or systems;

7 Unauthorized use or overflight of Unmanned Aerial Vehicle (UAV) on or over DOE property or facilities that have been designated as restricted air space (e.g., no-drone zone);

8 Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

(b) Category B MI IOSCs require notification to the ODSA. Examples include, but are not limited to:

1 Peaceful demonstrations (of over 20 persons or otherwise generating regional media attention or impacting operations);

2 Activities (brought to the attention of the IOSC Program) which draw negative media attention to a site's security operations;

3 Any use of force by Protective Force personnel in accordance with DOE O 473.2, current version;

4 Unauthorized use or overflight of Unmanned Aerial Vehicle (UAV) on or over DOE property or facilities which are not designated as restricted airspace; or

5 Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

(3) PI.

(a) Category A PI IOSCs are significant failures to adhere to security procedures (i.e., noncompliances) but do not result in the loss, theft, compromise or potential compromise of the asset. However, these noncompliances are significant enough to warrant notification to the ODFSA (in SSIMS). Examples include, but are not limited to:

1 Any unauthorized discharge of a firearm, pyrotechnic, or explosive (i.e., for other than training purposes or intentionally firing at hostile parties);

2 Any knowing, willful, or grossly negligent action to classify or continue the classification of information contrary to federal requirements;

3 Any knowing, willful, or negligent action to create or continue a special access program contrary to federal requirements;

4 Willful noncompliances (i.e., deliberate violations) with requirements for the protection of classified information (which do not result in loss, compromise, or potential compromise); or

5 Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

(b) Category B PI IOSCs are procedural noncompliances which do not result in the loss, theft, compromise or potential compromise of the asset.

1 These IOSCs must be supported by evidence (in the final IOSC report) that the asset was not compromised or the likelihood of compromise was remote.

2 Not all procedural noncompliances are inherently Category B PI IOSCs, only those procedural noncompliances specified in this Attachment and the IOSC Program Plan must be reported as IOSCs. Examples include, but are not limited to:

a The improper handling, and/or storage of classified matter.

b The improper processing or transmission of classified matter on unauthorized computer systems/networks (e.g., encrypted unmarked

classified information transmitted to only cleared personnel on government-furnished equipment, applications, or networks not authorized to process classified).

c UCNI was handled contrary to Physical Protection Requirements specified in 10 CFR 1017 Subpart E (e.g., failure to: notify of UCNI protection requirements, maintain physical control while in use, store in a manner to preclude unauthorized access, or destroy using authorized means).

d An unsecured door (or other boundary) for a security area authorized for the storage, access, or processing of classified matter or SNM.

e Unauthorized access (e.g., circumvention of access control requirements/controls) into a security area authorized for the storage of classified matter or SNM.

f Any negligent action that results in the misclassification of information. (Misclassification that results in compromise will be handled in accordance with applicable SI reporting requirements.)

g Intrusion Detection System (IDS) failure without appropriate Protective Force response or implementation of other authorized compensatory measures (where IDS is required).

h Diversion of accountable quantities of Cat III or IV quantity of SNM or any other circumstance resulting in Cat III or IV SNM (or other nuclear material controlled and accounted for as SNM in accordance with DOE O 474.2, current version) in an unauthorized (but Federally controlled) location (if there are no indications of malicious intent).

i Failure to obtain appropriate approvals for Foreign National access to DOE facilities, information, technologies or equipment (that is not administratively corrected after the fact).

j Improper issuance or termination of a DOE security credential (i.e., Personal Identity Verification [PIV] badge).

k Any unapproved controlled article which poses a threat to classified matter (e.g., a controlled article in close proximity to classified discussions, matter, or processing); in accordance with DOE O 473.1, current version, and as specified in the IOSC Program Plan.

l Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

4. PRELIMINARY INQUIRY, CATEGORIZATION, AND REPORTING REQUIREMENTS.

a. The preliminary inquiry and categorization are based on the requirements of this Attachment and any additional criteria as documented in the IOSC Program Plan. Preliminary reporting and categorization specifications include:

(1) The "clock" for IOSC categorization and the Initial IOSC Notification Report starts when the IOSC Program (i.e., an inquiry official) is notified of a PIOSC. Once the IOSC Program is informed of a PIOSC, they have a maximum of five (5) business days to:

(a) Perform the preliminary inquiry;

(b) Categorize the IOSC; and

(c) Perform any necessary initial reporting.

(2) Although a maximum of five (5) business days are provided, IOSCs must be categorized as soon as possible and the initial IOSC Notification Report must be made immediately (i.e., the same day) upon categorization.

(3) The categorization process is formally complete once the initial IOSC Notification Report is submitted.

(4) If there is still uncertainty at the five-business day mark, with respect to IOSC categorization, the IOSC must be reported at the highest appropriate Category pending completion of the inquiry process. If the final inquiry reveals additional details and facts, the IOSC can be re-categorized (e.g., from a Category A to a Category B, from a Category A to a non-IOSC, from a Category B to a non-IOSC, from a Category B to a Category A).

(5) The ODFSA may approve extensions to the five business-day categorization/initial notification report requirement. The IOSC Program Plan must specify the circumstances in which extensions may be requested (e.g., complicated Classification Program reviews) and the process for obtaining them.

(6) The IOSC Program Plan must describe the process in which PIOSCs are referred to the IOSC Program.

(7) Containment (i.e., mitigation) of events which involve suspected compromise must be initiated as soon as possible during the preliminary inquiry to avoid further compromise or additional damage to national security.

(8) The IOSC Program Plan must describe how containment activities are coordinated with applicable stakeholders (e.g., how Cybersecurity is engaged for spillages).

(9) Each IOSC must be assigned a unique local tracking number.

(10) The main emphasis for MI IOSCs is on notification; therefore, the subsequent section dealing with inquiries and closure reports is not applicable (unless additional information is requested by the ODFSA or ODSA).

b. Category A Reporting Requirements.

(1) The ODFSA must be notified of all Category A IOSCs.

(2) The initial IOSC notification report for Category A IOSCs must be submitted in SSIMS; if SSIMS is unavailable, the ODFSA must be appropriately notified within the designated timeframe, and SSIMS must be updated as soon as possible (e.g., on the next business day).

(3) The IOSC Program Plan must contain the notification content and process to include the roles, positions (e.g., personnel), or organizations identified for notification and any additional and/or specific notification requirements.

(4) If the IOSC involves classified matter, the Departmental element with programmatic responsibility for the information must be identified. Notification must include whether origination was by another agency or foreign government and a description of the compromise or potential compromise. See "IOSC Closure" in this section for additional content considerations for the initial report.

(5) If the ODSA determines that an IOSC involves the loss, theft, compromise, or potential compromise of Top Secret, SCI, SAP, and/or RD Nuclear Weapon Data, the ODFSA must:

(a) Coordinate a formal review of the IOSC to determine whether it constitutes a "significant atomic energy defense intelligence loss."

(b) If it is determined that the IOSC meets the significant atomic energy defense intelligence loss criteria, the ODFSA must inform the Secretary of Energy to perform required notifications in accordance with 50 U.S.C. Section 2656.

(c) If the IOSC does not meet the criteria for a "significant atomic energy defense intelligence loss," the ODFSA must notify the ODSA if any additional assessment of the IOSC's impact is necessary (e.g., if the IOSC is associated with a violation of law, if the information was compromised to a wide audience).

c. Category B Reporting Requirements. While notification and reporting of Category B IOSCs does not extend beyond the ODSA, the approved IOSC Program Plan must document the internal notification process.

d. Reporting Willful Noncompliances. Regardless of an IOSC category or type, IOSCs (Category A or B) determined to be willful or deliberate in nature (as defined in this Attachment) must be reported in SSIMS.

e. Reporting to Cognizant Personnel Security Offices (CPSOs). IOSCs, regardless of category, may impact an individual's eligibility for credentials (e.g., HSPD-12) and access to classified information. Therefore, the results of an IOSC where one or more employees are found responsible must be reported to the CPSO. Reporting to the CPSO is independent of whether a security violation or infraction is issued. The (specific) process for reporting IOSC results to the CPSO must be documented in the IOSC Program Plan.

f. Reporting IOSCs Associated with Sensitive Programs. IOSCs involving activities or information associated with sensitive programs must follow the same initial reporting process (i.e., initial IOSC notification report) but must omit classified details which exceed the authorized classification levels of approved reporting systems (i.e., SSIMS, locally approved system). These programs include the SCI Programs, SAPs, the Technical Surveillance Countermeasures (TSCM) Programs, the Counterintelligence (CI) Programs, or other programs identified by the appropriate ODFSA. All subsequent reporting must be handled within the programmatic channels until the inquiry report has been closed within the sensitive program.

g. Other Multi-Program Reporting. An event that meets the criteria for reporting as an IOSC does not negate the responsibility to report through other related reporting chains. In addition, in some cases (e.g., suspected criminal activity, involvement of a foreign agent, certain deliberate or willful violations), IOSC activities must cease, and the event must be referred to the appropriate Federal entity (e.g., Intelligence Community, FBI, IG) prior to taking any other preliminary inquiry activities. The process for providing other stakeholders (e.g., Intelligence Community, FBI, IG) a "right of first refusal" must be specified in the IOSC Program Plan. If appropriate, IOSC activities may resume if and when the event is referred back to the IOSC Program. Other multi-program reporting

includes, but is not limited to:

(1) Per NSPM-32, *Establishing a Standardized Procedure for Reporting Presidential Critical Information Requirements*, dated 1-13-2021, certain "significant" (i.e., having an impact at a national level) security events may require near-immediate reporting to the DOE CEOC.

(a) Depending on the type of event, required notifications must occur within minutes of "discovery" to within 3 to 48 hours.

(b) "Discovery," means confirmation or high confidence that a significant (i.e., national level) event has occurred as outlined by thresholds documented within the IOSC Program Plan.

(c) Although a maximum of five (5) business days are allotted for the IOSC preliminary inquiry, categorization, and initial notification report, the IOSC Program Plan must specify how the ODFSA and other key stakeholders (e.g., Cybersecurity, ORPS) are immediately informed of potential issues requiring more prompt reporting consistent with NSPM-32 requirements.

1 Any NSPM-32 related reporting for an IOSC (or PIOSC) must originate from the ODFSA through their responsible Emergency Operations Center to the DOE/NNSA Office of Emergency Management.

2 The ODFSA must confirm the IOSC Program Plan accurately addresses current NSPM-32 reporting requirements. Examples of PIOSCs (or IOSCs) which, if "significant" could merit NSPM-32 reporting include:

a Significant breach or significant unauthorized disclosure of classified information, or CUI (e.g., widespread dissemination or publication of classified information to unauthorized individuals, events which result or may result in FBI engagement due to criminal implications, a breach of U.S. Government-held CUI [which includes NNPI and UCNI] impacting a large number of records). NSPM-32 requires reporting within 48 hours.

b Significant security event (e.g., IOSC, PIOSC) at a U.S. Government facility or property which involves confirmed active shooter, casualties due to nefarious activity, terrorist attack or credible indications of an imminent attack, credible threats of violence (e.g., bomb threat), violent

demonstrations or protests, or penetration or surveillance of U.S. government facilities by individuals with nefarious intent. NSPM-32 requires telephonic notification within the first several minutes of discovery and written/verbal notification within three hours of discovery.

c Any security event which generates (or may generate) significant national media attention. NSPM-32 requires written/verbal notification within three hours of discovery.

d Any security event which is likely to cause the loss of public trust in a U.S. Government department or agency. NSPM-32 requires written/verbal notification within 48 hours of discovery.

e Other NSPM-32 thresholds must be specified by the ODFSA and addressed in the IOSC Program Plan.

(2) Per DOE O 232.2, *Occurrence Reporting and Processing of Operations Information*, current version, events which affect both safety and security are reportable through ORPS.

(3) Per DOE O 151.1, *Comprehensive Emergency Management System* current version, events that are reportable under the provisions of DOE O 151.1, current version, must continue to be reported in accordance with that Order and this Attachment.

(4) IOSCs involving privacy information (e.g., Personally Identifiable Information [PII]), both electronic and hardcopy, must be reported by the cognizant Cybersecurity Program (i.e., Information Systems Security Manager [ISSM]) to the integrated Joint Cybersecurity Coordination Center (iJC3) in accordance with DOE O 205.1, *Department of Energy Cybersecurity Program*, current version.

(5) NNSA "Flash Reporting" procedures are not affected by requirements in this section.

(6) Per DOE O 475.1, *Counterintelligence Program*, current version, the geographically closest element of the Office of Counterintelligence/Office of Defense Nuclear Counterintelligence must be notified of security incidents involving any credible information that a foreign national or an agent of a foreign power is involved or that there are indications of deliberate compromise from a U.S. Federal or contractor employee. Appropriate notifications (i.e., FBI) will then be made in accordance with 50 U.S.C. Section 402a.

(7) Per DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, when an inquiry surrounding an IOSC establishes information indicating that fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement has occurred, the Office of the Inspector General must be notified.

(8) Per DOE O 205.1, *Department of Energy Cybersecurity Program*, current version, any cybersecurity related event involving a Federal government information system and classified information with a confirmed impact to the confidentiality, integrity or availability must be reported to the Information Assurance Response Center (IARC) by the cognizant Cybersecurity Program (i.e., ISSM).

(9) Whenever a compromise involves the classified matter of another Federal agency, the ODFSA must coordinate with the other government agencies (CSAs), as appropriate.

(10) Whenever a compromise involves the matter of a foreign government that requires protection (e.g., Confidential Foreign Government Information Modified Handling [C/FGI-Mod], classified Foreign Government Information), the ODFSA must coordinate with the U.S. Department of State and the foreign government as appropriate. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise.

(11) If a compromise of SCI has occurred, the Director, Office of Intelligence and Counterintelligence, must consult with the designated representative of the Director, Central Intelligence and other officials responsible for the information involved.

h. Special Reporting Situations (SRS). Under certain circumstances, related IOSCs that are anticipated to recur over a long period of time may be consolidated from a reporting and documentation perspective (e.g., classified information from a previously reported and closed IOSC is found again later; under certain circumstances this event does not require separate/additional IOSC reporting). While these situations may be handled on a case-by-case basis between the ODSA and the ODFSA with specific reporting plans documented in the approved IOSC Program Plan, the following SRS types and scenarios are also authorized.

(1) SRS Type 1: An event, reported to the IOSC program, in which additional matter is discovered that is related to a previously categorized IOSC, to include:

(a) Discovery of additional matter not known or found during the initial IOSC inquiry may be dispositioned as an SRS if the IOSC Program presents a rational justification to the ODFSA for why the additional matter was not discovered previously (e.g., additional matter is found because of different document names, unknown

recipients/possessors, widely disseminated matter for which discovery and sanitization of all related matter was impractical or further propagation could not have been reasonably prevented and, accordingly, does not require separate IOSC reporting).

(b) If the ODFSA disagrees with the ODSA determination that the prior efforts were reasonable and sufficient, the ODFSA must notify the ODSA that the event must be reported as a new (separate) IOSC.

(2) SRS Type 2: An event, reported to the IOSC program, in which an official update in classification guidance results in the discovery of information which is not protected appropriately in accordance with the new classification guidance (but may have been appropriate based on legacy determinations).

(a) If the cognizant Classification Officer determines that, at the time of creation of the matter, the information was appropriately classified based on classification guidance—or the interpretation of classified guidance—available at that time, or under-classified matter was the result of updated classification guidance, this justification may be presented to the ODFSA and the event may be dispositioned as an SRS.

(b) If the ODFSA disagrees with the cognizant Classification Officer's justification or if the cognizant Classification Officer concludes the DC's determination was not reasonable or the DC was not diligent in their effort to appropriately classify the information, the event will be categorized as a new IOSC.

(3) SRS Type 3: An event in which a proactive search for potentially under-protected classified matter in specific topical area is considered warranted and may result in the discovery of improperly secured matter. Proactive searches may be conducted utilizing internal, network-based search tools specifically developed for this purpose, or a person or group tasked for this purpose. In situations where multiple items (e.g., documents) are discovered as a result of these searches, the ensuing events may be reported as a single IOSC under the following conditions:

(a) A proactive search requires the ODSA to submit a formal plan to the ODFSA.

1 The ODFSA must approve the plan before a proactive search can begin.

2 The plan must include the reason or driver for the search, location of the search, specific phrases or terms used during the search, and the timeframe of the search.

(b) Initial discovery of under-protected or classified documents resulting from the search will be categorized as one overarching IOSC (category and type as determined by the ODSA or ODFSA and as documented in the IOSC Program Plan).

(c) If a search reveals a new compromise or potential compromise, under-protected matter, or classified matter outside the pre-determined location(s), unapproved search terms or phases, and/or information collected outside the pre-determined timeframe, the ODFSA may require reporting a new IOSC.

5. CONDUCT OF INQUIRIES. An inquiry must be conducted to establish the pertinent facts and circumstances surrounding the IOSC. The specific inquiry process established by the ODSA must be documented in the IOSC Program Plan. Specific requirements and actions that must be considered when conducting inquiries include:

a. If an IOSC affects more than one site under the purview of a single Program and/or Site Office, that office must assign responsibility to a lead organization. If the sites fall under the purview of multiple Program Offices, those offices must, by mutual agreement, decide on a lead organization with responsibility for the inquiry and any reporting requirements.

b. In all instances where the ODFSA disagrees with the inquiry report, the ODFSA must assume supplemental inquiry responsibilities.

c. When the inquiry into an IOSC necessitates communication with agencies/ organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal, state, or local agencies), a federal employee is responsible for performing all such communication. The ODSA only performs this function with the written concurrence of the ODFSA.

6. INQUIRY OFFICIALS.

a. Inquiry officials must be either Federal or contractor employees and must have previous investigative experience or Departmental inquiry official training. Inquiry officials must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.

b. Inquiry officials must not detain individuals for interviews or to obtain sworn statements. Inquiry officials are authorized to conduct consensual interviews and request signed statements.

c. As part of their certification and training, all inquiry officials must complete and adhere to the legal requirements outlined in the DOE National Training Center online course, PMC-300DE, "Legal Aspects [of inquiries] Overview," (or successor training) to protect individuals' constitutionally protected rights.

d. Inquiry officials must be appointed in writing by the ODFSA.

e. If an inquiry official determines or suspects that a foreign power or an agent of a foreign power is involved, the inquiry official must stop further inquiry actions and notify the ODFSA, who will assume further notification and reporting responsibilities to include coordination with the Office of Counterintelligence. In such instances, the inquiry official must document the known circumstances surrounding the IOSC and submit all accumulated data to the ODFSA. The IOSC Program Plan must address how these events are handled.

f. If an inquiry official determines or suspects criminal conduct or another violation of law, the inquiry official must stop further inquiry actions and notify the ODFSA, who will assume further notification and reporting responsibilities to include coordination with appropriate law enforcement elements. In such instances, the inquiry official must document the known circumstances surrounding the IOSC and submit all accumulated data to the ODFSA. The IOSC Program Plan must address how these events are handled.

g. Personnel performing IOSC activities who are not yet formally certified or appointed as inquiry officials (i.e., in training) may support preliminary inquiry, inquiry, containment, and reporting activities under the oversight of a properly appointed inquiry official and as described in the IOSC Program Plan. Inquiry officials in training may not independently categorize IOSCs (or determine a PIOSC is a non-IOSC).

h. Inquiry officials are responsible for conducting the preliminary inquiry, initiating containment, completing the inquiry, submitting required notifications and reports, and maintaining all associated documentation associated with the inquiry. Specific actions must at least include:

(1) Conduct preliminary inquiry and disposition (e.g., categorize) all PIOSCs referred to the IOSC Program.

(2) Identify applicable stakeholders in accordance with the IOSC Program Plan and submit Initial Notification Report.

(3) Initiate containment and other mitigation activities for suspected compromises with applicable stakeholders (e.g., Cybersecurity) as soon as possible.

(4) Promptly notify the IOSC Program/s of other sites impacted by the event (e.g., classified information inappropriately transmitted to/from another National Laboratory).

(5) Collect and appropriately maintain all information and physical evidence associated with the IOSC.

(6) Identify persons associated with the IOSC and conduct interviews to obtain additional information regarding the IOSC.

(7) Identify responsible person or persons and determine whether security infractions or violations are warranted. In cases where a responsible person cannot be identified, the inquiry official briefs, as appropriate, the ODSA and other stakeholders to identify the most appropriate individual to implement any necessary corrective actions to prevent recurrence.

(8) Although inquiry officials are not responsible for recommending or issuing disciplinary actions, in accordance with the IOSC Program Plan, the inquiry official must document whether any administrative or disciplinary actions were taken against employees as a result of a security violation or infraction.

(9) Reconstruct the IOSC to the greatest extent possible using collected information and evidence. This includes developing a chronological sequence of events that describes the actions preceding and following the IOSC.

(10) Identify any collateral effect to other programs or security assets.

(11) Analyze and evaluate which systems/functions performed correctly or failed to perform as designed. This action will provide the basis for determining the cause of the IOSC and subsequent corrective actions.

(12) In accordance with IOSC Program Plan, work with appropriate stakeholders to determine the relevant cause/s and assist with the development of corrective actions to prevent recurrence.

(13) Develop and submit the final IOSC closure report.

7. IOSC CLOSURE. The final IOSC (closure) report serves as the basis for closing IOSCs and formally documenting the circumstances and context of the IOSC. This includes identifying the who, what, where, and when (and why, where required) of an event as well as any other contributing factors. Similar to inquiries, the level of detail provided in the report will vary based on the category and other factors (severity, asset, etc.) surrounding the IOSC (i.e., graded response). The report content and closing procedures must be documented in the IOSC Program Plan. At a minimum, the final closure report content and closure process must include:

a. Category A IOSC Closure:

(1) Category A IOSCs will be considered "closed" upon completion of inquiry activities and identification of proposed corrective actions which must be documented in the IOSC (closure) report in SSIMS.

(2) The ODSA or ODFSA, as appropriate, must be notified of IOSC closure in SSIMS.

(3) Category A IOSC closure documentation must include a cause analysis

and identification of accompanying proposed corrective actions.

(4) Category A IOSC corrective actions must be tracked to completion.

(5) The final closure report for Category A IOSCs must be submitted (i.e., closed) in SSIMS within 90 calendar days of the initial IOSC notification report. Extensions to the 90-day closure requirement must be approved by the ODFSA and submitted through SSIMS Status Update. The time frame for completing inquiries, process for seeking extensions, and process for reporting and closing IOSCs if SSIMS is unavailable must be addressed in the IOSC Program Plan. IOSCs not closed in SSIMS within 90 calendar days (or a 90-day extension) must continue to receive ODFSA-approved 90-day extensions until closed in SSIMS. In cases where SSIMS availability precludes on-time closure, the IOSC must be closed in SSIMS as soon as reasonably possible (e.g., next business day).

(6) Specific processes for documenting closure must be contained in the IOSC Program Plan.

(7) At a minimum, the final IOSC report for Category A IOSCs must include:

(a) The name of the individual(s) who was primarily responsible for the IOSC, including a record of prior IOSCs for which the individual had been determined responsible. Alternatively, why an individual was not determined responsible or could not be determined;

(b) A description of the intent (i.e., culpability) of the responsible individual(s) (i.e., inadvertent, negligent, grossly negligent, willful) and whether any disciplinary or administrative action was taken (e.g., security infraction, security violation);

(c) A description of the applicable causes;

(d) A description of the corrective actions proposed to preclude recurrence (the process for tracking corrective actions to completion and validating the effectiveness of those actions must be documented in the IOSC Program Plan);

(e) Specific reasons for reaching the conclusion that the loss, theft, compromise, or potential compromise occurred or was not remote;

(f) Identification of any collateral (i.e., extent of condition) effect to other programs or security assets;

(g) If the IOSC involves the compromise or potential compromise of information, the extent of the dissemination (e.g., number of

individuals and their citizenship; global disclosure via cyber mediums, open-source publication) must be identified; and

(h) Identification of specific impacts (i.e., degree of damage) of the IOSC to the Department and/or national security. Whenever an IOSC involves classified matter or assets of more than one Government agency, each agency is responsible for assessing the impacts resulting from its compromised matter.

b. Category B IOSC Closure:

(1) Category B IOSCs can be closed using SSIMS or a locally approved system identified in the IOSC Program Plan.

(a) The final Category B IOSC (closure) report must contain supporting documentation of factors used to determine that the likelihood of compromise and/or the potential for damage to national security is remote (e.g., failure to secure a document in a security container; however, multiple physical protection layers exist preventing unauthorized disclosure).

(b) This documentation provides the basis for making a statement that the circumstances surrounding the IOSC are such that the possibility of damage to the national security can be discounted.

(2) As appropriate, a description of applicable causes and (proposed) corrective actions to prevent recurrence.

8. DISCIPLINARY AND ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an IOSC must be assigned to an individual rather than to a position or office. When individual responsibility cannot be established and the facts show that a responsible official (e.g., project manager, director) allowed conditions to exist that led to an IOSC, responsibility must be assigned to that official. In cases where a responsible person cannot be identified, an appropriate individual must be identified to implement any necessary corrective actions to prevent recurrence (however, this individual will not be considered "responsible" for causing the IOSC).

b. A security violation is both a method for characterizing a noncompliance (e.g., a violation of policies or requirements) as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:

(1) The IOSC resulted in the loss, theft, compromise or potential compromise of classified information or unauthorized dissemination of UCNI;

(2) The IOSC did not result in the loss, theft, compromise or potential

compromise but reasonably could be expected to and is the result of gross negligence or a willful act;

(3) Any knowing, willful, or grossly negligent action to classify or continue the classification of information contrary to federal requirements;

(4) Any knowing, willful, or negligent action to create or continue a special access program contrary to federal requirements; or

(5) The IOSC is reported as a Category A SI and one or more responsible persons are identified.

c. A security infraction is both a method for characterizing a noncompliance that did not result in a violation (i.e., loss, theft, compromise or potential compromise did not occur), as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:

(1) Classified information was mishandled;

(2) UCNI was mishandled; or

(3) "Misuse" of U-NNPI.

d. Although inquiry officials are not responsible for recommending or issuing disciplinary actions, the IOSC Program Plan must specify or reference (local) policies that provide for appropriate administrative or disciplinary actions taken against employees who are responsible for security violations or infractions.

e. The IOSC Program Plan must document (e.g., reference other local procedures) how security violations and infractions will be tracked in order to identify patterns of negligence or carelessness or identify potential insider threats.

f. The final IOSC report must include a statement of whether any administrative or disciplinary actions were taken against a responsible employee (or employees). If an administrative or disciplinary action is taken, the final report must indicate whether one or more of the following factors applied:

(1) Involved a deliberate disregard (i.e., gross negligence or willful) of security requirements.

(2) Involved gross negligence in the handling of security assets (e.g., classified information, UCNI, SNM).

(3) Was not deliberate in nature but reflects a recent or recurring pattern of questionable judgment, irresponsibility, negligence, or carelessness.

g. Any administrative or disciplinary actions imposed on both cleared or uncleared individuals must be communicated to the respective personal identity verification office for Homeland Security Presidential Directive-12 (HSPD-12). The IOSC

Program Plan must document the process for communicating administrative actions to the HSPD-12 verification office (e.g., through local access control or badging offices).

ATTACHMENT 7
S&S PROGRAM MANAGEMENT OPERATIONS DEFINITIONS

This Attachment provides information associated with DOE O 470.1A and information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted.

1. GENERAL. This Attachment contains terms that are commonly used in the DOE S&S Program. Terms specific to an Attachment are also defined in that Attachment.

   a. Access Authorization. For purposes of classified visits by individuals from Other Government Agencies (OGA) other than DoD, NASA, and NRC, access may be granted to a cleared individual who has an official government need to access Restricted Data (RD) or Special Nuclear Material (SNM) as defined in the Atomic Energy Act of 1954, as amended. This access does not require conversion of the prospective visitor's existing security clearance to a DOE L or Q access authorization, provided that: an authorized DOE official has 1) verified the individual's CSA security clearance through DOE and national-level personnel security electronic databases, and 2) made a need-to- know determination with respect to the specific RD to be disclosed during the visit. The individual has executed an acknowledgement of receipt of a briefing on safeguarding RD, other classified information, and SNM (e.g., DOE F 5631.18, *Security Acknowledgement*).

   b. Classified Contract. Classified contract means any contract, license, agreement, or grant requiring access to classified information by a contractor and its employees for performance. A contract is referred to in this rule as a "classified contract" even when the contract document and the contract provisions are not classified.

   c. Classified Information. Information that is classified by statute or Executive order. Such information includes: (1) RD or FRD classified by the Atomic Energy Act or 10 CFR part 1045; (2) TFNI classified by the Atomic Energy Act; and (3) NSI classified by E.O. 13526 or prior Executive orders.

   d. Classified Matter. Anything in physical form that contains or reveals classified information.

   e. Classified Visit. A visit that will involve or is expected to involve access to, or an exchange of, classified information.

   f. Cleared Entity. A Federal government organization or contractor company that has been properly vetted and granted access to security assets and engage in security activities.

   g. Cognizant Security Agency (CSA). Cognizant security agencies (CSAs) are the agencies E.O. 12829, sec. 202, designates as having NISP implementation and security responsibilities for their own agencies (including component agencies) and any entities and non-CSA agencies under their cognizance. The CSAs are:

Department of Defense (DoD); Department of Energy (DOE); Nuclear Regulatory Commission (NRC); Office of the Director of National Intelligence (ODNI); and Department of Homeland Security (DHS)

h. Cognizant Security Office (CSO). The Federal government oversight office assigned responsibility for a given security program or function. Throughout this Order, the term "CSO" represents a DOE and/or NNSA Federal government oversight office. For the purposes of this Order, the term CSO is used to represent the Federal oversight offices identified in 32 CFR 117, listed below. The CSO may also conduct Industrial Security Services.

(1) Headquarters Office of Security Operations (EHSS)

(2) Office of Personnel and Facility Clearances and Classification (NNSA)

(3) Office of Naval Reactors (NNSA)

(4) Idaho Operations Office (NE)

(5) Pacific Northwest Site Office (SC)

(6) Richland Operations Office (EM)

(7) Savannah River Operations Office (EM)

i. Contractor. Any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination by a CSA. This term also includes licensees, grantees, or certificate holders of the USG with an entity eligibility determination (or FCL) granted by a CSA. The term "contractor" includes the prime contractor and subcontractors at all tiers and does not refer to contractor employees or other personnel.

j. Contractor employee. An individual employed by a Contractor as defined in this Attachment.

k. Controlled Unclassified Information (CUI). As defined in DOE O 471.7, CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a LRGWP requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

l. Controlling Agencies. Controlling agency is an agency that owns or controls the following categories of proscribed information and thus has authority over access to or release of the information: NSA for Communications Security Information (COMSEC); DOE for Restricted Data (RD); and ODNI for Sensitive

Compartmented Information (SCI).

m. Entity. Entity is a generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a subcontractor, subsidiary, or other subordinate or connected entity (referred to as "sub-entities" when necessary to distinguish such entities from prime or parent entities), a specific location or facility, or the headquarters/official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible CSA's procedures. The term "entity" as used in this part refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or subordinate organization.

n. Entity Eligibility Determination (EED). An assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity would be accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs also assess whether the entity is eligible for access to that category. Some CSAs refer to their favorable determinations as facility clearances (FCL). A favorable entity eligibility determination does not convey authority to store classified information.

o. Facility. A facility consists of one or more security interests under a single security management responsibility or authority and a single facility security officer within a defined boundary that encompasses all the security assets at that location. A facility operates under a security plan that allows security management to maintain daily supervision of its operations, including day-to-day observations of the security program.

p. Facility Clearance (FCL). Also called an "Entity Eligibility Determination (EED)." An administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or TS classified information, and allows access to proscribed information and other security assets.

q. Facility Security Officer (FSO). a U.S. citizen employee, who is cleared as part of the FCL. The FSO supervises and directs security activities necessary to implement NISP requirements, applicable requirements of this Manual and related

Federal requirements for classified information. The FSO, or those otherwise performing security duties, must complete security training as determined by the CSA.

r. Finding. A factual statement of identified issues and deficiencies (failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement) in the S&S program at a facility, resulting from an inspection, survey, self-assessment, or any other S&S review activity.

s. Foreign national. A person without U.S. citizenship or nationality (may include a stateless person).

t. Foreign Ownership, Control, or Interest (FOCI). A U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of a classified contract.

u. Government Contracting Activity (GCA). An agency component or subcomponent to which the agency head delegates broad authority regarding acquisition functions. A foreign government may also be a GCA.

v. Highest Material Balance Area. As defined in DOE Order 474.2, current version.

w. Incident of Security Concern (IOSC). An action (or inaction) contrary to S&S requirements and which meets DOE reporting requirements because it poses a threat to national security or DOE security assets (e.g., property, personnel, information, capabilities). IOSCs are categorized based on significance as A (more significant) or B (less significant) and type. The IOSC type is based on whether compromise or loss occurred; Security Interest (SI), loss or compromise occurred or is suspected, Procedural Interest (PI), a procedural noncompliance that did not result in loss or compromise, or Management Interest (MI), an IOSC reported primarily for management awareness. In addition to regulatory reporting requirements, Procedural Interest and Security Interest IOSCs require a formal inquiry to mitigate the effects and determine the nature, cause, impact, extent, and corrective actions to prevent recurrence.

x. Industrial Security Service Provider (ISSP). For the purposes of this Order, an ISSP is an organization or office that has been delegated authority by the Program Secretarial Officer or the CSO to render facility clearances, FOCI determinations, and/or perform other industrial security-related services on behalf of the CSO.

y. Initial Survey. A comprehensive review of the security status at a facility that is a candidate for an FCL, conducted to determine whether the facility in question meets established standards for the protection of the security interests and activities to be covered by the FCL.

z. Insider Threat Program Senior Official (ITPSO). The official an agency head or entity designates with responsibility to manage, account for, and oversee the agency's or entity's insider threat program, pursuant to the National Insider Threat Policy and Minimum Standards. The ITPSO is designated as a KMP that must be cleared in connection with the FCL.

aa. Key Management Personnel (KMP). As determined by a CSO, an entity's senior management official (SMO), facility security officer (FSO), insider threat program senior official (ITPSO), and all other entity officials who either hold majority interest or stock in or have direct or indirect authority to influence or decide issues affecting the management or operations of the entity or classified contract performance.

bb. Officially Designated Federal Security Authority (ODFSA). Federal employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. Delegation of ODFSA authority for these positions is originated according to direction from the accountable Program Secretarial Officer (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Officer), who also provides direction for which of the ODFSA positions may be further delegated. Each delegation must be documented in writing. It may be included in other security plans or documentation approved by or according to direction from the accountable principal. Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation.

cc. Periodic Survey. A survey conducted for all cleared facilities in accordance with established schedules that covers all applicable topics to meet the objectives of the S&S survey.

dd. Program Secretarial Officer (PSO). Headquarters Assistant Secretaries, Deputy Administrator, and Directors who have management responsibility for program planning, budgeting, and execution of DOE/NNSA mission program activities.

ee. Proscribed Information. information that is classified as top secret (TS) information; communications security (COMSEC) information (excluding controlled cryptographic items when un-keyed or utilized with unclassified keys); Restricted Data (RD); special access program information (SAP); or sensitive compartmented information (SCI).

ff. Reciprocity. If an entity has an appropriate, final entity eligibility determination, a CSA will not duplicate the entity eligibility determination processes performed by another CSA. An entity may be subject to duplicate processing when DOE cannot acknowledge obtain EED, FCL, or FOCI information and involved CSA.

gg. Safeguards and Security Activity. Also called Security Activity, is any work performed under contract, subcontract, or other agreement which involves accessing, receiving, generating, reproducing, storing (possessing and safeguarding), transmitting, and/or destroying security assets by the Department, a

Departmental contractor, or any other activity under the Department's jurisdiction. Security activity also includes the verification of such capabilities of approved Federal facilities and entities.

hh. Safeguards and Security (S&S) Interest(s). A general term for any Departmental resource or property that requires protection from malevolent acts. It includes but is not limited to Federal and contractor personnel; classified information and/or matter; sensitive compartmented information facilities; automated data processing centers; facilities storing, processing, and transmitting classified information and/or matter; vital equipment; special nuclear material (SNM); other nuclear materials; certain radiological chemical or biological materials; Unclassified Controlled Nuclear Information (UCNI), Controlled Unclassified Information (CUI); or other Government property of a significant monetary value (suggested threshold of $5 million).

ii. Self-Assessment. An internal integrated evaluation of all applicable S&S topical and sub-topical areas at federal or contractor sites to determine the overall status of the S&S program at that location and verify that S&S objectives are met.

jj. Senior Management official (SMO). The person in charge of an entity. Under the CCIPP, this is the authorized executive official with authority to sign the security agreement with DHS.

kk. Site. One or more entities (e.g., facilities, programs, organizations) operating under a centralized security management, with consolidated authority and responsibility for the security operations and typically covered by a site security plan. As used in this Order, refers to federally operated or contractor- managed locations, offices, departments, or programs.

ll. Subcontract. Contracts awarded to contractor entities, other than the Primary contractor, with performance activities that directly or indirectly support the overarching performance of the prime contract.

mm. Survey. An integrated performance and compliance-based evaluation of all applicable topics to determine the overall status of the S&S program at a facility or site and to ensure that S&S systems and processes at the location are operating in compliance with Departmental and national-level policies, requirements, and standards. Surveys are conducted or supervised by Federal security personnel.

nn. Suspected Compromise. Information is provided which indicates a compromise may have occurred, but no clear confirmation exists. A local inquiry reviews the circumstances to determine whether a potential compromise or (actual) compromise occurred. A suspected compromise is not a final determination of compromise status.

oo. Termination Survey. A survey of a cleared facility conducted to verify the termination of Departmental activities and the appropriate disposition of S&S interests at that facility. The termination survey confirms that all S&S activities

have been terminated or awarded to another contractor, that access authorizations have been properly terminated or dispositioned, and that no DOE property, classified information or matter, and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat remains.

pp. Visitor. An individual who is not an employee or contractor of the facility/site and does not work full or part-time at the facility/site.

ATTACHMENT 8
S&S PROGRAM MANAGEMENT OPERATIONS REFERENCES

This Attachment provides information associated with DOE O 470.1A and information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.1A) is inserted. Refer to the current version of listed References, or the current document for up-to- date requirements and programmatic information.

1. GENERAL. Terms commonly used in the DOE Safeguards and Security Program are defined in the DOE PIR tool located at https://pir.doe.gov/. In addition to these definitions, the following are provided:

   a. Public Law 115-232, The John S. McCain National Defense Authorization Act for Fiscal Year 2019.

   b. 10 U.S.C. Section 2536, Award of certain contracts to entities controlled by a foreign government: prohibition.

   c. 42 U.S.C. Chapter 23, Atomic Energy Act of 1954, as amended.

   d. 42 U.S.C. Sections 2011 to 2296, Atomic Energy Act of 1954, as amended. Establishes authorities and programs related to atomic energy, including programs for Federal control of the possession, use, and production of nuclear energy and SNM whether owned by the U.S. Government or others.

   e. 42 U.S.C. Section 2282b (Section 234B, as amended), establishes civil penalties for violations of directives regarding protection of classified information by contractors or their employees.

   f. 50 U.S.C. Sections 2406 and 2511

   g. 42 U.S.C. Section 2455(b) (Section 304[b] of the National Aeronautics and Space Act of 1958).

   h. 42 U.S.C. Section 5801, 5877 and 307, Energy Reorganization Act of 1974, requires investigating suspected, attempted, or actual thefts of special nuclear materials in the licensed sector and developing contingency plans for dealing with such events.

   i. 42 U.S.C. Sections 7101 to 7352, Department of Energy Organization Act, as amended. Establishes DOE and its basic authorities and responsibilities, including the responsibility of the Secretary of Energy for developing and promulgating DOE security policies.

   j. 10 CFR Part 1016, Safeguarding of Restricted Data by Access Permittees, requires the permittee to report any infractions, losses, compromises, or possible compromise of Restricted Data.

   k. 10 CFR Part 1017, Identification and Protection of Unclassified Controlled

Nuclear Information [UCNI], implements section 148 of the Atomic Energy Act which prohibits the unauthorized dissemination of UCNI, establishes minimum physical protection standards for UCNI, and established a procedure for the imposition of penalties on persons who violate section 148 of the Atomic Energy Act or 10 CFR part 1017.

l. 10 CFR Part 1045, Nuclear Classification and Declassification. Establishes the program for managing, identifying, generating, reviewing, and declassifying Restricted Data (RD), Formerly Restricted Data (FRD), and Transclassified Foreign Nuclear Information, and the sanctions for violations of the procedures. Part 1045.25 addresses the sanctions for knowing, willful, or negligent actions contrary to the requirements of the CFR that results in the misclassification of information.

m. 32 CFR Chapter XX, Information Security Oversight Office, National Archives and Records Administration. Establishes implementation requirements and procedures for classified national security information and the National Industrial Security Program.

n. 36 CFR Chapter XII, Subchapter B, Records Management. Establishes requirements for the creation, maintenance, and disposition of Federal records and penalties for unlawful or accidental removal, alteration, or destruction of records.

o. 32 CFR 117, National Industrial Security Program Operating Manual (NISPOM). Implements policy, assigns responsibilities, establishes requirements, and provides procedures, consistent with E.O. 12829, National Industrial Security Program; E.O. 10865, Safeguarding Classified Information within Industry; 32 CFR part 2004, for the protection of classified information that is disclosed to, or developed by contractors of the U.S. Government (USG).

p. 32 CFR Part 2001, Classified National Security Information. Prescribes requirements for Classified National Security Information.

q. 32 CFR Part 2004, National Industrial Security Program. This part sets out the National Industrial Security Program (NISP) governing the protection of agency classified information released to Federal contractors, licensees, grantees, and certificate holders.

r. 48 CFR Chapter 9, Department of Energy Acquisition Regulation. Supplements 48 CFR Chapter 1, Federal Acquisition Regulation (FAR), and includes the security provisions and clauses to be used in DOE solicitations and contracts when a facility clearance and/or access to classified information will be necessary for the performance of the contract. Includes the security clauses to be used in DOE solicitations and contracts or agreements involving access to classified information and/or a significant quantity of special nuclear material (SNM).

s. 48 CFR 52.204–2, [FAR] "Security Requirements" clause

t. Executive Order (E.O.) 12344, Naval Nuclear Propulsion Program

u. E.O. 12829, National Industrial Security Program. Establishes the National Industrial Security Program to protect classified information released by Federal agencies to their contractors.

v. E.O. 12968, Access to Classified Information. Prescribes requirements for access to classified information.

w. E.O. 13526, Classified National Security Information. If the Director of the Information Security Oversight Office finds that a violation of this policy or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

x. E.O. 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities.

y. E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, current version.

z. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

aa. Presidential Policy Directive-21, Critical Infrastructure Security and Resilience, current version. Establishes a national policy advancing a unified effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

bb. Directive-Type Memorandums (DTM) issued by the Office of the Under Secretary of Defense are available at https://www.esd.whs.mil/DD/DoD-Issuances/DTM/. DTMs may be issued periodically on a variety of topics. They do not automatically impose requirements on DOE but may contain useful information applicable to existing NISP programs.

cc. DCSA ISLs are available at https://www.dcsa.mil/mc/ctp/tools/. ISLs do not automatically impose requirements on DOE but may contain useful clarifications of existing NISPOM provisions.

dd. DOE Policy (P) 226.1, Department of Energy Oversight Policy, current version. Establishes a department-wide oversight process to protect the public, workers, environment, and national security assets effectively through continuous improvement.

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

ff. DOE Order (O) 142.3, Unclassified Foreign National Access Program, current version.

gg. DOE O 205.1 Department of Energy Cybersecurity Program, current version,

enables accomplishment of DOE mission to fulfill Federal cybersecurity requirements and protect DOE information systems. Establishes policy for incident response and reporting requirements for events impacting DOE information systems.

hh. DOE O 206.1, Department of Energy Privacy Program, current version. Establishes Departmental implementation of agency statutory and regulatory requirements for privacy, specifically those provided in the Privacy Act of 1974, as amended, and Office of Management and Budget directives.

ii. DOE O 221.1, Reporting Fraud, Waste and Abuse to the Office of Inspector General, current version. Establishes requirements and responsibilities for reporting fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement to the DOE IG.

jj. DOE O 226.1, Implementation of Department of Energy Oversight Policy, current version. Implements the policy that establishes a department-wide oversight process to protect the public, workers, environment, and national security assets.

kk. DOE O 227.1, Independent Oversight Program, current version. Prescribes the requirements and responsibilities for the Department's Independent Oversight Program to ensure the program is implemented in a transparent, efficient, and constructive manner to support the safe and secure accomplishment of DOE's missions.

ll. DOE O 243.1, Records Management Program, current version. Sets forth requirements and responsibilities for implementing and maintaining a cost-effective records management program throughout the Department of Energy.

mm. DOE O 414.1, Quality Assurance, current version. Ensures that the quality of DOE/NNSA products and services meets or exceeds the customers' requirements and expectations.

nn. DOE O 452.7, Protection of Use Control Vulnerabilities and Designs, current version. Establishes the policy, process, and procedures for control of sensitive use control information in nuclear weapon data (NWD) categories Sigma 14 and Sigma 15 to ensure that dissemination of the information must be restricted to individuals with valid need to know as well as IOSC reporting requirements.

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

pp. DOE O 470.3, Design Basis Threat [DBT], current version, defines DOE's physical protection strategies as well as National Security Assets and their associated protection levels (PLs).

qq. DOE O 470.4, Safeguards and Security Planning, current version, establishes Departmental Safeguards and Security Planning requirements and responsibilities.

rr. DOE O 470.5, Insider Threat Program, current version.DOE O 470.6, Technical

Security Program, current version.

ss. DOE O 471.1, Identification and Protection of Unclassified Controlled Nuclear Information [UCNI], current version. Provides requirements and responsibilities for identifying and protecting against the unauthorized dissemination of UCNI.

tt. DOE O 472.2, Personnel Security, current version.

uu. DOE O 473.1, Physical Protection Program, current version. Establishes requirements for the DOE Physical Protection (PP) Program for assets under the control of DOE. Includes protection requirements for Protection Level (PL) assets.

vv. DOE O 474.2, Nuclear Material Control and Accountability, current version. Establishes requirements for developing, implementing, and maintaining a nuclear material control and accountability (MC&A) program within DOE, including the NNSA, and for DOE-owned materials at other facilities that are exempt from licensing by the Nuclear Regulatory Commission (NRC).

ww. DOE O 475.1, Counterintelligence Program, current version. Establishes the Counterintelligence (CI) Program requirements and responsibilities for the DOE, including the NNSA, pursuant to Executive Order 12333 in order to detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity. Includes requirements to conduct investigations and inquiries of CI or counterterrorism concerns.

xx. DOE O 475.2, Identifying Classified Information, current version. Establishes the program to identify information classified under the Atomic Energy Act (i.e., Restricted Data [RD], Formerly Restricted Data [FRD], Transclassified Foreign Nuclear Information [TFNI]) or E.O. 13526, Classified National Security Information.

yy. DOE O 483.1, DOE Cooperative Research and Development Agreements, current version.

zz. DOE O 486.1, Foreign Government Sponsored or Affiliated Activities, current version.

aaa. Additional information and specific requirements for use of CPCI are set forth in the WebCPCI User's Guide that is available to all individuals authorized access to the system.