U.S. Department of Energy
Washington, DC

ORDER

DOE O 470.4C

Approved: 12-18-2024

SUBJECT: **SAFEGUARDS AND SECURITY PLANNING**

1. PURPOSE. To establish the U.S. Department of Energy (DOE) Safeguards and Security (S&S) Planning requirements and responsibilities. The requirements identified in this Order and its attachments are based on national policy promulgated in laws, regulations, Executive Orders (EOs), and national standards issued to prevent unacceptable adverse impacts on national security, the health and safety of DOE and contractor employees, the public, and the environment.

   DOE is a primary member of the Interagency Security Committee (ISC), established by EO 13286. The ISC's mandate is to enhance the quality and effectiveness of security in, and the protection of, buildings and non-military Federal facilities in the United States (U.S.). DOE implements the principles of the ISC Standards through the Department's S&S directives program.

2. CANCELS/SUPERSEDES. The portions of DOE O 470.4B Chg. 3 (LtdChg), Safeguards and Security Program, dated 9-23-2021, that relate to S&S Planning are hereby cancelled. DOE O 470.1A, Safeguards and Security Program Management Operations, cancels the S&S Management Operations portions of DOE O 470.4B Chg. 3

   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) that have been incorporated into a contract remain in effect throughout the term of the contract unless the contract or regulatory commitment is modified. This would either eliminate requirements that are no longer applicable or substitute a new set of requirements.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 Departmental elements. The Administrator of the National Nuclear Security Administration (NNSA) must ensure NNSA employees comply with responsibilities under this directive. This directive will not interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65, *National Defense Authorization Act for Fiscal Year 2000*, to establish Administration-specific policies, unless disapproved by the Secretary.

   b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the CRD, Attachment 1, sets forth requirements of this Order applicable to contracts that include the CRD or its requirements.

The CRD or its requirements must be included in all site, facility, and activity management contracts. Heads of field elements and Headquarters Departmental elements must identify contracts that should incorporate the CRD and notify contracting officers (CO) to incorporate the CRD into those contracts. COs are responsible for incorporating the CRD into the affected contracts as appropriate. COs must contact the Office of Security prior to modifying or excluding requirements from this Order in contracts to ensure national-level requirements or unacknowledged security risk is not inappropriately granted or accepted.

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

c. Equivalencies/Exemptions. Equivalencies and exemptions to this Order are processed in accordance with DOE O 251.1, Departmental Directives Program, current version.

(1) When conditions warrant equivalencies or exemptions from the requirements in this Order, requests must be supported by a Vulnerability Assessment (VA) or a security Risk Assessment (SRA) when required by the assets being protected, or by sufficient analysis to form the basis for an informed risk management decision.

(2) The analysis must identify compensatory measures, if applicable, or alternative controls to be implemented and the anticipated duration of the equivalency or exemption.

(3) Security risk must be accepted in accordance with authorities defined in DOE O 470.3, *Design Basis Threat (DBT) Order*, current version.

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

(5) Existing equivalencies and exemptions must be reviewed to determine applicability under DOE O 470.4C.

(a) If the requirement and the rationale have not changed, the equivalency or exemption remains valid.

(b) The review must be documented and approved by the Officially Designated Federal Security Authority (ODFSA) and does not need to be resubmitted for consultation or further approvals, unless directed by the responsible Program Office.

(6) The organization seeking a formal equivalency or exemption from S&S requirements within DOE O 470.4C must obtain advice from the Office of Primary Interest and their relevant General Counsel office before submitting the request for approval. The Office of Security must respond to consultation requests within 45 business days from the receipt of the request.

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

(8) Naval Reactors. In accordance with the responsibilities and authorities assigned by EO 12344, Naval Nuclear Propulsion Program, codified at 50 U.S.C., War and National Defense, 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. S&S planning programs within this Order must be developed, maintained, and incorporated in the responsibilities and requirements section contained in this Order and its associated attachments.

b. S&S planning must be thoroughly integrated with other Departmental programs to ensure DOE mission accomplishment.

c. S&S planning must incorporate a risk-based approach to protect assets and activities against the consequences of acts that may have an adverse impact on national security or the environment, or that may pose danger(s) to the health or safety of DOE Federal or contractor employees or the public as defined in DOE O 470.3, current version.

d. S&S Planning must address site-specific characteristics and requirements, current technology, programs, and operational needs to achieve levels of system effectiveness or the levels of system effectiveness established by the security risk accepted by the authorities defined in DOE O 470.3, current version, in a cost-effective manner.

e. Delegation of S&S Authorities.

(1) Delegation of authority to 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 Office) 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.

f. Implementation.

(1) After being notified by the Head of the Departmental Element or designee, the CO must incorporate the CRD in Attachment 1 in existing applicable contracts per the process described in DOE O 251.1, 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 plan must be submitted to the appropriate Cognizant Security Office (CSO), prior to this deadline.

(a) The implementation plan 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.

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

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Ensures effective S&S Program Planning is established and executed within DOE under the authorities granted by the Atomic Energy Act, as amended (42 U.S.C. sections 2011 to 2286), relevant EOs; the U.S. *Department of Energy Organization Act*, as amended (42 U.S.C., *The*

Public Health and Welfare, sections 7101 to 7352); and, and in accordance with P.L. 106-65, the *National Nuclear Security Administration Act*.

(2) Designates senior Departmental officials to direct and administer the S&S Program.

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

(4) Designates DOE program elements responsible for ensuring foreign nationals' visits requiring access to classified information are conducted in accordance with governing international agreements or treaties.

b. Deputy Secretary.

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

c. Under Secretary of Energy for Nuclear Security and Administrator of 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) Through the Associate Administrator and Chief for Defense Nuclear Security:

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

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

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

(1) Develops and promulgates the Department's S&S policy consistent with strategies and policies governing the protection of national security and other critical assets entrusted to the Department and in accordance with laws, regulations, and national-level policies and standards.

(2) Responsible for the DOE Headquarters S&S Program, including the development of S&S plans and procedures and guidance for programs described in this Order.

(3) Provides advice and assistance to DOE organizations concerning S&S planning described in this Order.

(4) Acts as the senior Agency official responsible for the direction and implementation of and compliance with EO 12829, , section 203(a), and 32 CFR 117, *National Industrial Security Program Operating Manual*, excluding NNSA, pursuant to EO 12829, section 203(a).

(5) Maintains national-level liaison with Federal law enforcement, security, and intelligence agencies in support of DOE S&S Program Planning. Represents DOE in interagency efforts related to S&S activities.

(6) Periodically reviews IAEA guidance documents, e.g. Nuclear Security Series – Fundamentals, Recommendations, and Implementing Guidance, when developing DOE safeguards and security policy.

e. DOE Line Management.

(1) DOE line management refers to the chain of responsibility that extends from the Secretary of Energy to the Deputy Secretary, to the Secretarial Officers who set program policy and plans and develop assigned programs, and to the program and Field Element Managers or ODFSAs who are responsible for execution of these programs.

(2) Commits resources, directs the allocation of personnel, and approves implementation plans and procedures in the performance of specific work activities.

f. Heads of Departmental Elements.

(1) Provide guidance and oversight to ensure S&S Planning Programs under their cognizance are adequately implemented, managed, and maintained.

(2) Designates DOE (CSOs) under their purview.

(3) Delegates authority to the ODFSA or ODSA.

(4) Administers assigned S&S programs or functions delegated to them.

g. Heads of Field Elements/Offices.

(1) Administer the program planning requirements for the purposes of protecting S&S interests.

(2) Ensures COs incorporate the CRD into applicable contracts.

h. Officially Designated Federal Security Authority.

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

(2) Ensures S&S Awareness Program activities are accomplished for facilities and sites under their cognizance.

(3) Ensures Survey and Self-Assessment Program activities are accomplished for facilities and sites under their cognizance.

(4) Ensures S&S Training Program activities are accomplished at facilities and sites under their cognizance.

(5) Approves site security plans (SSPs) and facility security plans, as applicable.

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

(7) Approves analysis used in security planning for assets that do not require VAs or SRAs in accordance with the DBT.

(8) Approves performance assurance plans.

(9) Approves compensatory measures.

(10) Approves reviews of existing equivalencies and exemptions to determine applicability under.

i. Officially Designated Security Authority.

ODSAs execute requirements and responsibilities that are formally delegated from DOE or NNSA.

j. Director, 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 S&S training programs and provides S&S training to Departmental personnel through the National Training Center (NTC).

(4) Establishes the Department's Training Approval Program (TAP) and Job Analysis for S&S programs.

k. Contracting Officers.

(1) Upon notification of applicability, incorporate the CRD into existing applicable contracts via the appropriate process for the contract type without delay.

(2) Assist originators of contract solicitations to incorporate the requirements of this Order, as applicable.

(3) COs must consult with the Office of Security prior to modifying or withholding any requirements in this Order from a contract.

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

7. DEFINITIONS. See Attachment 7.

8. REFERENCES. See Attachment 8.

9. CONTACT. Questions concerning this Order should be addressed to the Office of Security Policy, Office of Environment, Health, Safety and Security at Security.Directives@hq.doe.gov. Formal clarification requests should be submitted to the Director, Office of Security through the respective Program Office.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

ATTACHMENT 1.
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 470.C, *SAFEGUARDS AND SECURITY PLANNING*

This Contractor Requirements Document (CRD) establishes Safeguards and Security (S&S) planning requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration contractors.

Regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments 2, 3, 4, 5, and 6 to DOE O 470.4C referenced in and made a part of this CRD, which provide program requirements and/or information applicable to contracts in which this CRD is inserted.

ATTACHMENT 2.
SECURITY PLANS AND ANALYSIS

This Attachment provides requirements associated with DOE O 470.4C and requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4C) is inserted.

1. GENERAL.

   a. All DOE facilities and sites or contractor facilities with DOE security assets (reference DOE O 470.3, current version) must have a security plan approved by the ODFSA.

   b. The security plan serves as the approved authorization basis for security operations and must account for assets, site-specific operations, S&S program implementation at that location, and security risks associated with operations under the security plan.

   c. Security plans must provide assurances for safeguarding against loss, theft, diversion, unauthorized access, misuse, or sabotage of radioactive materials and radioactive sealed sources that could adversely affect national security and the health and safety of employees, the public, and the environment in accordance with DOE O 470.3, current version, DOE O 231.1, *Environment, Safety and Health Reporting*, current version, and 10 CFR Part 835, *Occupational Radiation Protection*, Subpart M and Appendix E.

   d. DOE site Federal line management, in consultation with contractor security managers as applicable, will determine and define the facilities under their cognizance and how or if a group of facilities will be consolidated into the security plan. This includes non-possessing subcontractors. This decision is made locally to facilitate the security management at each location. Facility security plans can be used for the purpose of documenting and managing facility-specific security requirements.

2. ASSESSMENTS AND ANALYSES. The security plans must be based on an analysis of considerations specific to the location, to include local and regional input to the threat assessments, and the consequences of loss or misuse of assets and interests to be protected. For assets that require Vulnerability Assessments (VA) or Security Risk Assessments (SRA) as specified in the Design Basis Threat (DBT), the analyses must be completed in accordance with the DBT and the results documented.

   a. For assets that do not require VAs or SRAs, analysis must be performed in accordance with ODFSA approved methodologies based on considerations specific to the location; consequences of loss or misuse of the assets; security measures in place; DBT and local threats; identification of risk; and compliance to requirements. The results of the analysis must be documented.

3. SECURITY CONTINGENCY PLANNING. This section replaces the former security conditions program. Each DOE site must have plans and procedures that address integration and communication between various organizations/programs (e.g., security, counterintelligence, emergency management, fire, and medical departments) to address responses to real-time and potential (predicted) security and non-security events.

   a. Non-security events include hazards identified in the all-hazards planning basis in accordance with DOE O 151.1, *Comprehensive Emergency Management System*, current version. These events must be coordinated with the emergency management organization to determine the need to invoke security measures differing from or above the baseline security program.

   b. Each DOE site must plan for events/hazards and establish procedures that support the rapid implementation and deployment of pre-determined security contingency measures, such as the closure of select site and/or facility entry points; reduced site access; increased and/or more rigorous inspections; modified Protective Force deployment schemes and staffing for surveillance and response; increased support from local, state, tribal, and federal resources; supplemental protections; etc.

   c. Consideration must be given to actionable measures when protective actions (including evacuation, take cover, or shelter in place) are required for an event posing an imminent threat to workers and potential recovery actions when protective actions are lifted.

4. SECURITY PLAN COMPONENTS. The plan must describe in detail, either in its content or in combination with other explicitly referenced procedures (i.e., implementing instructions), all aspects of S&S operations occurring at the location. A key component of the security plan is they type of asset requiring protection, the strategy to protect the assets, the specific Protective Force positions (numbers), and systems that must be maintained in operable condition to implement the strategy. The security plan must include:

   a. Overview of Site and mission.

   b. Prioritized list of all DBT assets and facilities and associated protection strategies.

   c. Organizational structure, to include roles and responsibilities of Federal employees and contractors, delegations of authority, and integration with other functional areas (i.e., safety, emergency management, counterintelligence, etc.).

   d. List of exemption/equivalencies to include process for review and approval.

   e. Identification of analyzed security risk and/or system effectiveness with the supporting Federal line management approval. The associated analyses must be described or referenced.

f. Results of the special nuclear material (SNM) roll-up credibility analyses and, when applicable, the supplemental security measures to prevent roll-up. The associated analyses must be described or referenced.

g. The life cycle cost analysis process used to support the timely replacement of security structures, systems, and components.

h. Contractual security requirements to include the contract modification procedure.

i. Procedures providing security requirements for outside users, entities, etc. that conduct activities at a Departmental site.

j. Description of how changes to the security plan (i.e., authorization basis) are addressed, approved, and managed.

k. List of applicable and approved memorandums of understanding/ agreements.

l. Description of security areas, to include the associated security measures.

m. All requirements identified in other Departmental directives or guidance that are required to be included in the security plan.

n. Description of how all security topical areas and Departmental requirements are implemented (plans and procedures), to include tactical doctrine, demonstrator/ protestor plans, etc.

o. Current implementation plans for meeting changes in S&S policies or other changes (such as the addition or removal of security interests) that will exceed the implementation timeline specified in the relevant policy.

p. Document the process the ODFSA uses to complete required approvals. If other required approvals are completed through approval of the SSP, the SSP must explicitly state which documents are approved by this process.

q. Facility Security Plans must be included via reference, if applicable.

5. SECURITY PLAN REVIEWS AND UPDATES.

a. The security plan and supporting analyses must be reviewed and the following changes must be incorporated into the security plan. The ODFSA must approve these changes prior to implementation. If there are no changes, the security plan must be minimally reviewed and documented on an annual basis.

(1) Changes in facility operators/contractors.

(2) Changes in baseline security requirements in applicable national-level or DOE policy.

(3) Changes in risk or the authorization basis.

(4) Planned changes to the security program at the facility or site.

(5) Changes directed by DOE line management.

(6) Changes in operations to include (but not limited to) addition of assets, modification of assets, or asset removal not covered by security plans at a facility or site that require modification to approved security measures.

b. The site must determine if temporary or permanent changes are within or beyond the scope of the current authorization basis. If it is beyond the scope, then ODFSA approval is required prior to implementation. When appropriate, determinations should be supported by analyses.

ATTACHMENT 3.
PERFORMANCE ASSURANCE

1. GENERAL.. Protection programs must ensure assets are protected in compliance with Departmental and site-specific requirements as identified in the site's security plan and commensurate with the protection strategies and threats defined in DOE O 470.3, current version. The intent of the performance assurance program is to monitor and assess the health of the protection programs by evaluating the collective set of available data, to include, but not limited to testing, assessments, incidents of security concern, findings, data sets, etc. The goal is not to duplicate assurance activities specified in this and other Orders, but rather to leverage all assurance activities to monitor the health of the security programs. Additionally, the performance assurance program identifies if security measures across the various security programs warrant designation as essential elements; thereby, requiring additional testing requirements (i.e., system effectiveness test) and compensatory measures when performance is degraded.

2. PURPOSE. A performance assurance program must identify and establish monitoring and testing activities to verify protection program elements are functioning as required.

   a. Activities and schedules for performance assurance must be included in the performance assurance plan.

   b. Performance assurance activities results must be evaluated to identify possible trends across security programs e.g., to determine if identified issues represent an isolated case or systemic problem.

   c. Corrective actions must be taken when degraded performance is identified for a security program.

3. ESSENTIAL ELEMENTS. The designation of essential elements was previously restricted to the physical security measures (e.g., the measures contributing in a significant way to Probability of Sensing, Probability of Assessment, Probability of Neutralization, Response Force Times, etc.) which were directly related to the protection of assets. Compliance-based programs, such as classified matter protection and control (CMPC), Human Reliability Program, and Operations Security (OPSEC), are also considered primary methods by which certain risks are addressed and may be considered essential elements as determined by site analysis. Security programs and the associated security measures must be evaluated to determine if they warrant designation as an essential element.

   b. Essential elements system effectiveness testing is required unless it is a compliance-based program.

   c. The testing of the essential element is not prone to failure or subject to compromise without noticeable tampering, such as walls and fences, as long as it can be documented that tampering with such elements would be detected in time to prevent compromise of overall protection.

4. COMPENSENTORY MEASURES. Compensatory measures must be implemented immediately when an essential element fails or is out-of-service.

   a. Compensatory measures must be evaluated for effectiveness and provide an equivalent level of protection.

   b. Compensatory measures must be approved by the ODFSA.

   c. Compensatory measures must be continued until maintenance is completed and the system is performance tested and returned to service.

   d. Compliance-based essential elements may not require compensatory measures.

   e. The ODFSA must be notified:

      (1) When compensatory measures are implemented.

      (2) When a security program, such as CMPC, HRP, Access Authorizations, OPSEC, is identified as an essential element and is affected by any condition that results in degradation of protection.

      (3) When a physical protection program element is affected by any condition that results in the degradation of protection.

5. PERFORMANCE ASSURANCE PLANNING. Sites must develop a performance assurance plan(s); the plan must:

   a. Be approved by the ODFSA.

   b. Define assurance activities for all S&S topical areas relating to Program Management Operations, Physical Protection, Protective Force, Information Security, Personnel Security, and Material Control and Accountability at the facility/site, relevant to protection of assets.

   c. Document the protection program elements and essential elements protecting assets as outlined in the security plan.

   d. Describe the assurance activities (performance test, self-assessment, etc.) associated with each protection program element, including type of test and frequency.

   e. Describe Performance Assurance activities for compliance-based programs. These programs may be assessed through surveys and self-assessments.

   f. Describe physical elements not subject to compromise without noticeable tampering, e.g., walls and fences, which are not required to be tested.

g. Describe the process for managing and tracking assurance activities, including the utilization of results and resolution of deficiencies.

h. Describe actions to be initiated in the event of any essential element failure.

6. TEST FREQUENCY.

a. Testing frequency must be based on manufacturer's recommendations, analysis, site-specific conditions, operational needs, or other DOE directives to ensure program effectiveness.

b. Systems, system components, and essential elements are performance tested at a frequency documented in the Performance Assurance Plan, and, at a minimum, annually.

7. ANALYSIS AND DOCUMENTATION.

a. Assurance activities and analysis results must be documented.

b. Issues requiring corrective action must be documented and tracked until resolved.

c. When an essential element is affected by any condition resulting in the degradation of protection, immediate compensatory measures must be implemented until the issue is resolved and performance testing confirms all applicable elements have returned to full operability.

8. REVIEWS AND UPDATES. Performance assurance plans must be reviewed and updated, when necessary, due to:

a. Changes in site mission, programmatic activities, or S&S interests and/or assets.

b. Changes in the operation or physical configuration of a facility or site, (building addition, new work processes or systems, construction of fences, roads, buildings, demolition of buildings, or reconfigurations of fences, roads, etc.).

c. Completion of S&S upgrades or downgrades.

d. Changes in protection strategy, risk, Protective Force deployment, or other revisions to the applicable SSP.

e. Changes in S&S policies.

ATTACHMENT 4.
SURVEY AND SELF-ASSESSMENT PROGRAMS

1. GENERAL REQUIREMENTS. Surveys and self-assessments are conducted to ensure compliance with Departmental and national-level S&S policies, requirements, and standards for the protection of DOE security assets

    a. DOE CSOs are responsible for the survey and self-assessment program for facilities and sites under their cognizance.

    b. The survey and self-assessment programs must be documented in security plans.

2. SURVEYS. Surveys are conducted to confirm that a Federal, government-owned contractor-operated, or contractor facility meets relevant security requirements and to inform Federal line management of the effectiveness of the facility security program. Surveys also help to identify issues or concerns with the security program, and to allow Federal managers to make informed decisions to manage risk. Additional information on FCLs may be found in DOE O 470.1 Program Management, current version.

    a. Initial Surveys: Possessing (safeguarding) facilities require a satisfactory initial survey as one of the conditions for granting the initial a facility security clearance (FCL).

    b. Periodic Surveys: Periodic surveys must be conducted for all applicable S&S topical areas (as identified in the DOE F 470.8 Survey/Inspection Report Form) at facilities maintaining an FCL.

        (1) The frequency, scope, and scale of Surveys are determined using a risk-based process.

            (a) The risk-based process must be documented.

            (b) The risk-based process must be ODFSA approved.

                1 Sites with classified information, SNM, or PL-5 assets must conduct a survey at intervals not to exceed every 36 months.

                2 Sites with any other security asset must conduct a survey conducted at intervals not to exceed every 48 months.

        (2) If a survey does not occur as scheduled, the reason for the delay must be communicated to the appropriate federal authority.

        (3) Periodic surveys of Federal entities with an FCL must be led by a Federal employee not assigned to the facility being surveyed.

(4) Periodic Surveys of government-owned contractor-operated or contractor facilities must be led by a Federal employee. These surveys must be independently developed, conducted, and reported to the appropriate Federal line management, e.g., Site Office to Program Office.

(5) The Office of Enterprise Assessment Multi-Topic Assessments may be used to meet the periodic survey requirement.

c. Special Surveys. Special surveys may be conducted at facilities for specific limited purposes, or at the direction of the CSO. Examples include but are not limited to extended survey activities; "for cause" reviews; line management direction; shipment of nuclear and/or classified information or matter; or a change in the contractor operating a government-owned facility.

d. Termination Surveys. When a possessing facility no longer requires an FCL, a termination survey and ensure that appropriate forms are submitted and SSIMS is updated to enact the termination. A termination survey must be conducted to verify the termination of security activities and the appropriate disposition of S&S interests.

(1) Termination survey activities include, verification of the appropriate disposition, destruction, or return of classified information or matter, SNM and/or Other Accountable Nuclear Material (OANM), hazardous material, or property; the signing of a certificate of possession if classified matter or information is to be retained by the contractor for the allowable period; security badge retrieval; and verification of debriefings or transfer of access authorizations to other DOE interests.

(2) Termination surveys must be conducted onsite at facilities possessing classified matter, Sensitive Compartmented Information or Special Access Program information or matter, or SNM and/or OANM.

(3) For all other facilities, termination surveys may be conducted either onsite or through any other means established by the CSO. Sites without FCL do not require a termination survey.

3. SELF-ASSESSMENTS. Self-assessments ensure compliance with all security requirements appropriate to the activities, information, and conditions at the location.

a. Self-assessments are required by both Federal and contractor entities by site designated personnel.

b. Self-assessments must be conducted between periodic surveys.

c. Self-assessments must be conducted at intervals not to exceed every 36 months.

(1) Contractor self-assessments at site/facilities with classified matter must be conducted annually in accordance with 32 CFR 117, National Industrial

Security Program Manual. These self-assessments must include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program.

(2) Reviews conducted by DOE federal entities or other federal agencies may be used to meet the annual self-assessment requirement, if conducted within the required timeframe.

(3) For non-possessing contracts, the contractor is responsible for flowing down assessment requirements to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with requirements.

d. Self-assessment reports must be provided to Federal line management.

4. REPORTS AND RATINGS.

a. A report for survey and self-assessment activities must be developed; the report must, for each applicable S&S topic and subtopic assessed, contain a description of the survey or assessment activities performed for each element; how the review was conducted, including any samples and tests used in the evaluation; a summary of the observations made, including findings, deficiencies, and non-compliant conditions; and an analysis of the results that support the ratings awarded.

b. The report must identify and provide a rationale for topics or subtopics that are not assessed or rated, e.g., when a topic or subtopic does not apply at a given facility.

c. Each topic or subtopic reviewed must receive a rating based upon the effectiveness and adequacy of the security programs at the facility being assessed. The ratings listed below must be used for all surveys and self-assessments.

(1) Satisfactory. The element being evaluated meets protection objectives or reasonable assurance that protection objectives are being met.

(2) Marginal. The element being evaluated meets SOME protection objectives but leaves some uncertainty or questions regarding the adequacy of how or questionable assurance that protection objectives are being met.

(3) Unsatisfactory. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

d. Surveys result reports must be entered into SSIMS.

5. FINDINGS AND CORRECTIVE ACTIONS.

a. Findings must cite a legal, regulatory, performance, compliance, or other applicable requirement.

b. All open S&S findings from any source (previous surveys and assessments; inspections, reviews, and reports by other organizations such as the Office of Enterprise Assessments, Government Accountability Office, or the Office of the Inspector General; etc.) must be reviewed during surveys to validate the status of corrective actions and to evaluate the impact on the current operation of the facility's S&S program. Findings closed during the survey period must be reviewed for sustainability of the closing action.

c. Findings from all surveys must be documented in the associated report and entered into SSIMS in accordance with guidelines issued by the SSIMS database manager.

(1) Contractors are not required to use SSIMS for findings from self-assessments, contractors may use internal issues management processes and tools.

(2) Findings must be tracked until closed and monitored on an established schedule to ensure that corrective action plans to address the issue are being implemented in a timely and effective manner.

d. Corrective action plans must be developed for all survey and self-assessment findings and must include action(s) which mitigate or preclude the recurrence of the issue that resulted in the finding.

(1) Corrective actions must include causal analysis of the extent of condition of the finding to determine whether it represents an isolated issue or is a systemic problem associated with a specific topical element, a specific facility or with the overall status of the S&S program.

(2) For all identified findings, corrective actions must be initiated in accordance with an approved issues management system. The effectiveness of corrective actions must be validated during subsequent surveys to ensure that the action taken has been sufficient to prevent recurrence of the issue that resulted in the finding.

(3) Corrective actions for surveys must be reported in SSIMS and changes to the status of the action must be reported in SSIMS until the associated finding is closed.

6. DOCUMENTATION. Reports of surveys, self-assessments, and review activities must be maintained in accordance with a valid National Archives and Records Administration, (NARA) approved federal records disposition schedule.

ATTACHMENT 5.
SAFEGUARDS AND SECURITY TRAINING PROGRAM

This section describes the requirements for establishing training for personnel working in S&S programs.

1. DOE Line Management must ensure that S&S training activities are accomplished for facilities and sites under their cognizance and that contractors under their cognizance accomplish their responsibilities under this program.

    a. The content of training must be documented and consistent with the knowledge, skills and abilities required to perform assigned S&S tasks and/or responsibilities as determined by job analyses.

    b. Federal employee training is addressed in DOE O 360.1, *Federal Employee Training*, current version.

2. Contractors must ensure that S&S training activities are accomplished at their respective facilities and sites. Procedures applicable to S&S training must be documented.

    a. An S&S training program must be documented for all personnel performing S&S tasks. The S&S training program for each facility must encompass all program elements which are performed by employees working at that location and must be reviewed annually. S&S tasks include any function, responsibility, authority assigned or required by DOE or national S&S policy. At a minimum, the training program must define the initial training requirements required for an individual to independently perform S&S responsibilities.

    b. The content of training must be documented and consistent with the knowledge, skills, and abilities required to perform assigned S&S tasks and/or responsibilities as determined by job or functional analyses.

        (1) The analysis must be based on S&S roles and responsibilities and site-specific mission requirements for each position.

        (2) At a minimum, the job or functional analysis should include the duties and tasks required to perform the job or function.

    c. Training must be designed using a systematic approach to training.

    d. Training can be provided by external sources, such as commercial vendors, or other government training agencies. Training products procured from these resources must be evaluated for consistency with DOE policy and needs.

    e. The DOE NTC TAP validates the site's systematic approach to training.

(1) TAP is a recommendation for S&S programs to ensure a local course development process for non-NTC training follows a formal systematic approach.

(2) The TAP does not apply to organizations that do not develop and/or deliver training.

f. Accurate and complete employee training records that contain dates of course attendance, course title, and scores/grades achieved (where applicable) must be maintained in accordance with a valid NARA approved federal records disposition schedule.

ATTACHMENT 6.
SAFEGUARDS AND SECURITY AWARENESS

This Attachment provides requirements associated with DOE O 470.4C and requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4C) is inserted.

1. PURPOSE. The S&S awareness program is responsible for communicating personal security responsibilities through briefings and supplemental awareness activities to all individuals at a facility or site.

2. GENERAL REQUIREMENTS. DOE line management is responsible for ensuring security awareness program activities are accomplished for sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program.

   Procedures applicable to the security awareness program must be documented in security plans.

   The security awareness program must:

   a. Ensure that security awareness briefings are conducted in accordance with the requirements of this section, for all covered individuals.

   b. Ensure that, if security awareness briefings are conducted through electronic means, a method must exist to verify the individual completes all required content prior to receiving credit for the briefing.

   c. Ensure that visitors granted unescorted access to a facility/site security area receive security awareness information (e.g., information on prohibited and controlled articles).

   d. Determine administrative actions to be taken when an individual fails to complete the requirement for annual refresher briefings.

   e. Ensure that all individuals granted DOE security clearances (access authorizations) execute a Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*, prior to being granted access to classified information or matter.

   f. Ensure that individuals are appropriately authorized to witness and accept the SF 312 on behalf of the U.S. and that such designations of authority are documented.

   g. Ensure that executed SF 312 forms and other records related to the security awareness program are maintained in accordance with a valid NARA approved federal records disposition schedule.

h. Ensure supplemental awareness materials are available to address local site conditions and issues for both cleared and non-cleared individuals and visitors, to make them aware of their security responsibilities.

3. BRIEFINGS. S&S awareness programs must include briefings for non-DOE personnel granted unescorted access; individuals with a DOE security clearance for access to classified information or matter, or SNM and/or OANM; individuals who are issued a DOE security badge (HSPD-12); and individuals terminating a DOE security clearance.

a. Initial Briefing. Individuals who receive a DOE security badge must receive an initial briefing to identify basic site-specific security responsibilities. Initial and comprehensive briefings may be combined at the discretion of the facility/site management. Under such circumstances, the briefing must include information prescribed for both initial and comprehensive briefings.

(1) Content. The content of the initial briefing must include the following items.

(a) Overview of the DOE facility/organization's mission.

(b) Overview of facility/organization's major S&S program responsibilities.

(c) Access control requirements.

(d) Escort requirements and procedures.

(e) Protection of Government property requirements.

(f) Badge responsibilities.

(g) Identification of controlled and prohibited articles.

(h) Controlled Unclassified Information protection responsibilities.

(i) Identification of classification markings.

(j) Procedures for reporting incidents of security concern.

(2) Scheduling.

(a) The initial briefing must be completed before personnel are given unescorted access to a site security area higher than General Access Areas.

(b) A transferred individual must complete a site-specific initial briefing before assuming duties at the new site.

(3) Documentation.

(a) Records must be maintained to verify an individual's completion of the briefing.

(b) Records may be maintained in conjunction with badging records or other records pertaining to access control.

b. Comprehensive Briefing. Individuals who are granted a security clearance must receive a comprehensive briefing to identify security responsibilities for access to classified information, or matter, Unclassified Controlled Nuclear Information (UCNI), or SNM and/or OANM, when applicable. Initial and comprehensive briefings may be combined at the discretion of the facility/site management. Under such circumstances, the briefing must include information prescribed for both initial and comprehensive briefings.

(1) The content for the comprehensive briefing must include the following items:

(a) Responsibilities for safeguarding classified information or matter SNM and/or OANM, or UCNI:

1 Purpose of DOE classification program.

2 Definition of classified information or matter.

3 Levels and categories of classified information or matter.

4 Damage criteria associated with each classification level.

5 Definition of SNM/OANM, to include the different categories/types of SNM/OANM as defined in DOE O 474.2A, current version.

6 Classification awareness information that covers at a minimum the content required in paragraph 1.b. of Attachment 6 to DOE O 475.2, *Identifying Classified Information*, current version.

7 Requirements for the protection of classified information or matter via telecommunications and electronic transmissions.

8 As applicable, UCNI awareness information that covers requirements to identify and protect UCNI from 10 CFR part 1017 and DOE O 471.1B, current versions.

9 Requirements for access controls, security badges, and security clearance levels.

10 Responsibilities associated with escorting and site-specific escort ratios.

11 Procedures for reporting incidents of security concern.

12 Legal and administrative sanctions for security infractions and violations of law.

13 Purpose and requirements of, and responsibilities for, the SF 312.

14 Definition and penalties of unauthorized disclosures.

(b) Personnel security requirements as contained in DOE O 472.2, *Personnel Security*, current version:

1 Purpose of the personnel security program.

2 Sources of legal authority and guidance.

3 Access authorization process.

4 Key terms associated with adjudications.

5 Adjudication factors.

6 Administrative Review.

7 Individual reporting requirements.

(c) Counterintelligence awareness requirements contained in DOE O 475.1, *Counterintelligence Program*, current version.

(2) Scheduling.

(a) Comprehensive briefings must be completed prior to being granted initial access to classified information or matter, or SNM.

(b) A comprehensive briefing may also be completed when a security clearance is shared or transferred to another DOE facility/site.

(3) Documentation.

(a) The SF 312 must be used to document the completion of the comprehensive briefing.

(b) The SF 312 may be used to document subsequent comprehensive briefings.

(c) Records must be maintained to verify an individual's completion of the briefing.

c. Refresher Briefing. Cleared individuals must receive an annual refresher briefing to reinforce the information provided in the comprehensive briefing.

(1) Content. The content for the refresher briefing must include the following items.

(a) Current site-specific security issues.

(b) Classification awareness requirements contained in DOE O 475.2, current version, as applicable.

(c) Counterintelligence awareness requirements contained in DOE O 475.1, current version.

(d) Individual reporting requirements as contained in DOE O 472.2, current version.

(e) As applicable, UCNI awareness information that covers requirements to identify and protect UCNI from 10 CFR part 1017 and DOE O 471.1B, current versions.

(2) Scheduling.

(a) Refresher briefings must be conducted at a frequency not to exceed 12-months.

(b) Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations receive refresher briefings on schedule.

(c) Failure to complete the annual refresher briefing by an individual who holds a security clearance will result in administrative actions determined by DOE Line Management, including possible administrative withdraw of the security clearance, until such time as the individual has complied with the briefing requirement.

(3) Documentation.

(a) Records must be maintained to verify an individual's completion of the briefing.

(b) Documentation must include the ability to identify individuals who have not met the refresher briefing requirements.

d. Termination Briefing. A cleared individual must receive a termination briefing to reiterate their continued responsibilities.

(1) Content. The content for the termination briefing must include:

Information contained in the numbered items of the Security Termination Statement (DOE F 472.12 or successor form).

Information contained in items 3, 4, 5, 7, and 8 of the SF 312; and

Penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy Act and pertinent sections of 18 U.S.C., *Crimes and Criminal Procedure*.

(2) Scheduling. The termination briefing must be conducted and reported when there is a termination of employment, a change of official duties, or any other change in circumstance such that the individual no longer requires access to classified information or SNM in accordance with DOE O 472.2, current version.

(3) Documentation. The completed DOE F 5631.29, *Security Termination Statement* (or successor form), must be used in accordance with DOE O 472.2, current version.

(4) Records must be maintained to verify an individual's completion of the briefing.

Records may be maintained in conjunction with badging records or other records pertaining to access control.

4. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT.

a. A cleared individual must execute an SF 312 after completing the comprehensive briefing and prior to being granted access to classified information or matter.

b. The SF 312 must be completed by hand or digitally signed.

(1) Departmental elements are permitted to accept hand signed SF 312 forms provided the following requirements are met.

(a) The employee must sign and date the SF 312 in the presence of a witness.

(b) The employee's and witness' signature must bear the same date.

(c) The same person may serve as both the witness and acceptor of the SF 312 if that person has been authorized to accept the signed form on behalf of the U.S.

(2) Departmental elements are permitted to accept digital signatures on the SF 312 provided the following requirements are met:

(a) Digital signatures must be based on public key infrastructure (PKI) and reliable certificate authority combination, such as a PKI and personal identity verification card requiring a personal identification number.

(b) If a user signs digitally, there is no need for a witness because of the authentication, consent, and integrity provided by the digital signature. As a result, the witness blocks on the SF 312 will not be filled out when the form is digitally signed.

(c) No other forms of e-signature are authorized.

(3) Any DOE Federal employee may witness the execution of the SF 312 by a government or non-Government employee.

(4) A DOE Federal employee specifically authorized to do so may accept on behalf of the U.S. an SF 312 executed by either an employee of DOE, contractor or subcontractor, whose clearance is granted by DOE.

(5) An authorized representative of a contractor who has been specifically designated to act as an agent of the U.S. may witness and accept an SF 312 executed by another DOE contractor/subcontractor employee.

(6) Report any refusal to execute the SF 312 to the DOE CSO and Cognizant Personnel Security Office within 48 hours.

c. Retention.

(1) The original executed SF 312 or a legally enforceable copy must be retained in accordance with a valid NARA approved federal records disposition schedule.

(2) The SF 312 or legally enforceable copy must be expeditiously retrieved if the U.S. Government seeks enforcement or subsequent employers require confirmation of execution.

(3) Personnel security files must not be used as a storage location for the agreements.

(4) Contractors supporting the creation and management of SF 312 forms on behalf of the DOE and its facilities must ensure all forms and

documentation are created in electronic format, with fully digital form fields and digital signatures, and managed to the appropriate NARA approved Federal Records Disposition Schedule.

(5) Upon an individual's termination of employment, the SF 312(s) must be sent to the CSO, in accordance with 32 CFR Part 2001.

5. SUPPLEMENTARY AWARENESS ACTIVITIES. Supplementary security awareness activities must be conducted to ensure that individuals, whether cleared or uncleared, are aware of their S&S responsibilities and good security practices.

a. Awareness activities must address general security concerns or be tailored to site-specific problems or issues as indicated by incident reports, employee questions, or management communications.

b. Awareness activities must be carried out in any form which meets the needs of the site, including but not limited to briefings, presentations, posters, newsletters, token items such as badge lanyards, employee recognition, computer notices, fliers, tabletop cards, etc.

ATTACHMENT 7. DEFINITIONS

This Attachment provides information associated with DOE O 470.4C as well as information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4C) is inserted.

Definitions for terms used in a general S&S context are available through the S&S Policy Information Resource tool at https://pir.doe.gov/.

1. 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. The CSO may also conduct Industrial Security Services.

    a. Headquarters Office of Security Operations (EHSS)

    b. Office of Personnel and Facility Clearances and Classification (NNSA)

    c. Office of Naval Reactors (NNSA)

    d. Idaho Operations Office (NE)

    e. Pacific Northwest Site Office (SC)

    f. Richland Operations Office (EM)

    g. Savannah River Operations Office (EM)

2. Essential Elements (EE). Protection and assurance elements necessary for the overall success of the S&S program at a facility or site, the failure of any one of which would result in protection effectiveness being significantly reduced; which would require performance of other elements to be significantly better than expected to mitigate the failure; or create an unaccepted increase in security risk. Essential elements can include but are not limited to equipment, procedures, and personnel. Compliance-based programs, such as CMPC, Human Reliability Program, and OPSEC, are also considered a primary method by which certain risks are addressed and may be considered essential elements.

3. Federal Record. Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business

4. Finding. Findings are the 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.

5. 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.

6. 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 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 Office), 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.

7. Officially Designated Security Authority (ODSA). Federal or contractor employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation.

8. Performance Testing. Performance tests ensure a system or component is performing as intended and is effective. These testing methods are used in a combination to analyze system effectiveness

9. Periodic Survey. A survey conducted for facilities in accordance with established schedules that covers all applicable topics to meet the objectives of the S&S survey.

10. Protection Program. Activities that protect Departmental property and personnel from adversary actions that would adversely impact national security and the health and safety of employees, the public, or the environment.

11. Protection Program Elements. Specific elements of a S&S protection program.

12. Records Schedule. A records disposition schedule is a legally binding document that tells you how long to keep specific types of federal records and what should happen to those records when they have met their retention requirement.

13. Safeguards and Security Awareness. A program that identifies required safeguards & security briefings for obtaining & maintaining a security clearance; administers the SF312 Classified Information Nondisclosure Agreements; includes other activities to educate or raise the awareness of individuals as to their responsibilities within the site security programs.

14. Safeguards and Security Training. The process of providing for and making available to an employee a planned, prepared, and coordinated program, system, or routine of instruction in S&S topical areas applicable to the employee's position that will improve individual and organizational performance and assist in achieving the Department's mission and performance goals.

15. Security Asset Categorization. The Department possesses assets of the highest national security importance, which must be protected by safeguards and security systems that can successfully meet the Design Basis Threat (DBT) requirements. The categories of these assets include:

    a. Nuclear explosives

    b. SNM of improvised nuclear device (IND) concern

    c. SNM of theft concern

    d. Chemical, biological, radiological material, nuclear material, and select agents and toxins of public health and safety concern

    e. National critical infrastructure

    f. Critical program assets or facilities

    g. Classified matter

    h. Controlled Unclassified Information (CUI)

    i. Government property

    j. Personnel

16. 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.

17. Site. A site consists of one or more facilities operating under a centralized security management, including a site security officer with consolidated authority and responsibility for the facilities, and covered by a SSP that may consolidate or replace, wholly or partially, individual facility plans.

18. Special Surveys. Surveys conducted for specific limited purposes. Examples include extended survey activities, technical security activities, "for cause" reviews, line management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a government-owned facility.

19. Survey. An integrated performance and compliance-based evaluation of all applicable topics to determine the overall status of the S&S program at a 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.

20. System Effectiveness Testing. System effectiveness of physical protection systems must be determined by performance testing of detection, assessment, delay and response

capabilities in concert. System effectiveness does not apply to any individual detection sensor but to all parts of the protection systems that work together in facilitating a response that mitigates the DBT adversary threat. System effectiveness is determined through performance testing, and analyzing the results, at a frequency as documented in the Performance Assurance Plan.

21. Security Risk Assessment (SRA). An evaluation to assess the order compliance protection strategy and protection strategy objectives of protection, mitigation, incident response, and mission recovery for PL-5 through PL-7 assets.

22. 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.

23. Vulnerability Assessment (VA). A systematic evaluation process in which qualitative and quantitative techniques are applied to identify vulnerabilities and to determine system effectiveness for an S&S system to protect specific assets from specific adversaries and their acts.

ATTACHMENT 8. REFERENCES

This Attachment provides information associated with DOE O 470.4C as well as information applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4C) is inserted.

1. 42 U.S.C. sections 2011 to 2296, *Atomic Energy Act of 1954*, as amended.

2. 42 U.S.C. sections 7101 to 7352, *Department of Energy Organization Act*, as amended.

3. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

4. 10 CFR Part 835, *Occupational Radiation Protection*, Subpart M and Appendix E

5. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*, current version.

6. 10 CFR Part 1045, *Nuclear Classification and Declassification*, current version.

7. 32 CFR 117, *National Industrial Security Program Operating Manual (NISPOM)*, current version.

8. 32 CFR Part 2001, *Classified National Security Information*, current version.

9. EO 12829, *National Industrial Security Program*, current version.

10. EO 13526, *Classified National Security Information*, current version.

11. PPD-21, *Critical Infrastructure Security and Resilience*, current version.

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

13. DOE O 231.1, *Environment, Safety and Health Reporting*, current version

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

15. DOE O 360.1, *Federal Employee Training*, current version.

16. DOE O 470.3, *Design Basis Threat (DBT) Order*, current version.

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

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

19. DOE O 471.6, *Information Security*, current version.

20. DOE O 472.2, *Personnel Security*, current version.

21. DOE O 473.1, *Physical Protection Program*, current version.

22. DOE O 474.2A, *Nuclear Material Control and Accountability,* current version.

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