U.S. Department of Energy

Washington, D.C.

ORDER

DOE O 470.7

Approved: 08-05-2026

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. PURPOSE. The Department of Energy (DOE) is modernizing its security framework. This update addresses rapidly evolving threats, changing mission needs, and advancing technology. The transition to a risk-based security operations (RBSO) approach aligns security resources—funding and personnel—with mission risk. This modernized strategy enhances protection effectiveness while enabling more flexible, mission supportive operations. The focus is on a risk-based approach to security for high-consequence categories of special nuclear material (SNM) and other accountable nuclear material operations. The objective is to replace prescriptive, one-size-fits-all methods with adaptable, risk-informed strategies that address evolving threats, control costs, and improve mission effectiveness. An RBSO program increases efficiency and removes unnecessary burdens, delays, and expenses that impede DOE/National Nuclear Security Administration's (NNSA's) national security missions, delivering the right security in the right place at the right time. The RBSO approach empowers the Head of Field Element or the Officially Designated Federal Security Authority (ODFSA), as appropriate, to make informed risk decisions based on security analysis and effects-based performance outcomes. The approach emphasizes continuous improvement, data-driven evaluation, and the achievement of defined security objectives, ensuring that operations are flexible, focused on managing risks and meeting clear performance standards.

2. CANCELS/SUPERSEDES. This Order cancels/supersedes DOE Order (O) 470.1A, 470.4C, 471.1B, 471.6, 471.7, 473.1A, 473.2A, and 474.2A for the facilities and activities specified in section 3. Cancelling a directive does not alter existing contractual or regulatory compliance obligations; Contractor Requirements Documents (CRD) in contracts remain effective until formally changed.

3. APPLICABILITY.

   a. Departmental Elements. This Order applies to all Departmental elements, including NNSA, and their associated field elements.[1]

      (1) The NNSA Administrator will ensure that NNSA employees and contractors comply with their respective responsibilities under this Directive.

[1] Operations offices, service centers, site offices, area offices, field offices, government-owned government-operated facilities, and regional offices of federally staffed laboratories that report directly to a DOE Headquarters office.

(2) Nothing in this Order shall be construed to limit or supersede the authority of the Administrator for Nuclear Security under 50 United States Code (U.S.C.) § 2402, Administrator for Nuclear Security, including the authority to establish Administration-specific policies unless disapproved by the Secretary. In the event of any inconsistency between this Order and the NNSA Act, the Act controls with respect to NNSA programs and activities.

b. DOE Contractors. The requirements of this Order shall be incorporated into applicable contracts, including Management and Operating contracts. The contractor is responsible for flowing down the requirements of this CRD, if applicable. Contractors shall comply with the requirements of applicable federal, state, and local laws and regulations in carrying out the requirements of this Order unless relief has been granted in writing. Omission of any applicable law or regulation from the Order does not affect the obligation of the contractor to comply with such law or regulation. Contractors must comply with the requirements of this Order, except to the extent modified by the equivalencies or exemptions identified herein or issued to the contractor in writing by DOE utilizing the process outlined in DOE O 251.1E, *Departmental Directives Program*, including as amended or updated.

c. Equivalencies and Exemptions.

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

(2) Exemption. This Order does not apply to activities regulated by the Nuclear Regulatory Commission (NRC) or by a State acting under an agreement with the NRC pursuant to the *Atomic Energy Act of 1954* (AEA), as amended.

(3) Other Equivalencies/Exemptions. Many DOE safeguards and security (S&S) Program requirements are based on regulations from federal agencies and codified in the Code of Federal Regulations (CFRs), Executive Orders (EOs), or Presidential Directives. To deviate from these, follow the process specified in the source document. If none exists, deviations require risk analysis, ODFSA approval with Program Office review, and consultation with the DOE Office of the General Counsel to confirm legal eligibility.

4. REQUIREMENTS. Additional S&S requirements are outlined in Attachments 1 and 2, as applicable.

   a. Delegation of S&S Authorities.

      (1) All delegations must be formally documented and issued in accordance with the office granting authority.

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

      (3) The acceptance of security risks is a fundamental federal responsibility and may not be delegated.

   b. Site Security Plan.

      (1) Each DOE facility subject to this Order must have a security plan that addresses site-specific security requirements and procedures, consistent with the applicable laws, regulations, Executive Orders, other national-level requirements, and DOE Directives. The security plan must also address the key contractor performance requirements provided in Attachment 2.

      (2) Contractor performance requirements will be defined in contractual language.

      (3) The Officially Designated Security Authority (ODSA) must submit a security plan to the ODFSA for review and approval.

5. RESPONSIBILITIES.

   a. Secretary of Energy.

      (1) Ensure an effective S&S Program is established and executed for the protection of SNM, sites, and other Departmental assets under the authorities granted by relevant Executive Orders; the Department of Energy Organization Act, as amended (42 U.S.C. § 7101, Definitions, to § 7352, Contents of review); and the *Atomic Energy Act of 1954*, as amended (42 U.S.C. §§ 2011 *et seq*.); and in accordance with P.L. 106-65, National Defense Authorization Act for FY 2000.

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

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

(4) Designate 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. The Deputy Secretary.

(1) Approve and implement S&S policies.

c. Program Secretarial Officer.

(1) Provide performance requirements, guidance, and oversight to ensure S&S planning programs under a Program Secretarial Officer's cognizance are adequately implemented, managed, and maintained.

(2) Designate DOE Cognizant Security Office (CSOs) under their purview.

(3) Delegate authority to the ODFSA.

(4) NNSA, through the Associate Administrator and Chief for Defense Nuclear Security acts as the Senior NNSA official responsible for the direction and administration of the NNSA implementation.

(a) 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.

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

d. Cognizant Security Offices. 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) Administer and oversee assigned S&S program management operations activities for their sites on behalf of the Program Secretarial Office.

(2) Industrial Security Service Providers render facility clearances (FCL), foreign ownership, control, or influence (FOCI) determinations, and other industrial security-related services on behalf of the CSO.

e. Heads of Field Elements.

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

(2) Administer program planning requirements for the purpose of protecting S&S interests.

(3) Ensure Contracting Officers incorporate the CRD into applicable contracts.

(4) Approve equivalencies to this Directive in consultation with the responsible Program Office.

f. Director, Office of Environmental, Health, Safety and Security.

(1) Act as the senior agency official responsible for the direction and administration of the DOE implementation of and compliance with the National Industrial Security Program pursuant to Executive Order 12829, National Industrial Security Program.

(2) Act as the senior agency official responsible for the direction and administration of the DOE information security program pursuant to Executive Order 13526, Classified National Security Information.

(3) Review site security plans for consistency with applicable requirements.

g. Officially Designated Federal Security Authority. ODFSAs are federal employees who possess the knowledge and responsibilities for each situation in which they are assigned through delegation.

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

(2) Fulfill responsibilities as defined in this Order.

(3) Approve site security plans and supporting analyses that protect assets under their cognizance.

(4) Accept or transmit the security risk for assets under their cognizance.

(5) Review and approve equivalencies for assets under their cognizance.

h. Officially Designated Security Authority. ODSAs are federal or contractor employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation.

(1) Execute those responsibilities formally delegated.

(2) Ensure security protocols are followed, exemptions and equivalencies are documented and approved.

(3) The ODSA must approve all subordinate documents incorporated within the security plan to ensure compliance with established security protocols and standards.

i. Cognizant Office of the General Counsel or Chief Counsel.

(1) Review site security plans for consistency with applicable laws, Executive Orders, regulations, and government-wide policies.

j. Contracting Officers.

(1) For all applicable contracts and upon notification that a site/facility management contract is affected by this Order, the contracting officer(s) shall incorporate the requirements into the affected contract(s) via the "Laws, Regulations, and DOE Directives" clause of the contract, or through negotiation and modification, as appropriate.

6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods unless specifically included in the references.

7. REFERENCES.

a. P.L. 90-618,Gun Control Act of 1968

b. P.L. 95-452, 92, Statute 1101, Inspector General Act of 1978, as amended

c. P.L. 111-272, Law Enforcement Officers Safety Act

d. P.L. 103-353, Uniformed Services Employment and Reemployment Rights Act of 1994

e. P.L. 114-328, National Defense Authorization Act, 2017

f. 10 U.S.C § 4874(a-b), "Award of certain contracts to entities controlled by a foreign government: prohibition"

g. 18 U.S.C. § 930, Possession of Firearms and Dangerous Weapons in Federal Facilities

h. 21 U.S.C. § 841, Prohibited Acts A

i. 42 U.S.C. § 5195c, Critical Infrastructures Protection

j. 42 U.S.C. §§ 2011–2296, The Atomic Energy Act of 1954, as amended

k. 42 U.S.C. § 2278a, "Trespass upon Commission installations"

l. 42 U.S.C. §§ 7101–7352, Department of Energy Organization Act, as amended

m. 50 U.S.C. §41, National Nuclear Security Administration

n. 50 U.S.C. § 2402, Administrator for Nuclear Security

o. 50 U.S.C. §2661, Protection of Certain Nuclear Facilities and Assets from Unmanned Aircraft

p. 7 CFR § 331, Possession, Use, and Transfer of Select Agents and Toxins, Security

q. 9 CFR § 121, Possession, Use, and Transfer of Select Agents and Toxins, Security

r. 10 CFR § 110, Export and Import of Nuclear Equipment and Material

s. 10 CFR § 707, Workplace Substance Abuse Programs at DOE Sites

t. 10 CFR § 710, Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material or Eligibility to Hold a Sensitive Position

u. 10 CFR § 712, Human Reliability Program

v. 10 CFR § 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations

w. 10 CFR § 851, Worker Safety and Health Program

x. 10 CFR § 860, Trespassing on Department of Energy Property

y. 10 CFR § 1016, Safeguarding of Restricted Data by Access Permittees

z. 10 CFR § 1017, Identification and Protection of Unclassified Controlled Nuclear Information

aa. 10 CFR § 1045, Nuclear Classification and Declassification

bb. 10 CFR § 1046, Medical, Physical Readiness, Training, and Access Authorization Standards for Protective Force Personnel

cc. 10 CFR § 1047, Limited Arrest Authority and Use of Force by Protective Force Officers

dd. 10 CFR § 1048, Trespassing on Strategic Petroleum Reserve Facilities and Property

ee. 10 CFR § 1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve

ff. 29 CFR § 1910, Occupational Safety and Health Standards

gg. 32 CFR § 117, National Industrial Security Program Operating Manual (NISPOM)

hh. 32 CFR § 2001, Classified National Security Information

ii. 32 CFR § 2002, Controlled Unclassified Information (CUI)

jj. 41 CFR § 102-74, Subpart C, "Conduct on Federal Property"

kk. 42 CFR § 73, Select Agents and Toxins, Security

ll. 42 CFR § 1003, Possession, Use, and Transfer of Select Agents and Toxins

mm. 48 CFR § 904.70, "Facility Clearance"

nn. 48 CFR § 952, Solicitation Provisions and Contract Clauses

oo. 49 CFR § 173, Shippers–General Requirements for Shipments and Packaging

pp. EO 10865, "Safeguarding Classified Information Within Industry"

qq. EO 12344, "Naval Nuclear Propulsion Program"

rr. EO 12829, "National Industrial Security Program"

ss. EO 12968, "Access to Classified Information," as amended

tt. EO 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," as amended

uu. EO 13526, "Classified National Security Information"

vv. Homeland Security Presidential Directive (HSPD)-12, "Directive on Policy for a Common Identification Standard for Federal Employees and Contractors"

ww. Presidential Memorandum for Heads of Executive Departments and Agencies, subject: Tracing of Firearms in Connection with Criminal Investigations, dated January 16, 2013

xx. National Archives and Records Administration General Records Schedule (GRS) 5.6, "Security Records"

yy. National Security Memorandum (NSM)-22, "Critical Infrastructure Security and Resilience," 2024

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

aaa. DOE O 206.2, *Identity, Credential, and Access Management*, current version

bbb. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*

ccc. DOE 452.8, *Control of Nuclear Weapon Data*

ddd. DOE O 470.6, *Technical Security Program*, current version

eee. DOE O 472.2A, *Personnel Security*, current version

fff. DOE O 475.2B, *Identifying Classified Information*, current version

NOTE: *Whenever a legal, regulatory, or other external standard, or a DOE Policy, Order, Notice or Manual is referenced, and such standard is amended or superseded, the successor standard is applicable under this Order. DOE Orders referenced in this Order can be located on the DOE Directives webpage, https://www.directives.doe.gov/.*

8. DEFINITIONS. Terms used in the DOE Safeguards and Security programs are defined and located on the Policy Information Resource website, http://pir.doe.gov.

9. CONTACT. Address inquiries to the Cognizant Program Office.

BY ORDER OF THE SECRETARY OF ENERGY:

JAMES P. DANLY
Deputy Secretary

ATTACHMENT 1, CHAPTER I
CONTRACTOR REQUIREMENTS DOCUMENT SAFEGUARDS AND SECURITY PROGRAM

This Contractor Requirements Document (CRD), which includes the requirement in Attachment 2, specifies key, measurable performance requirements for Safeguards and Security by Department of Energy (DOE) and National Nuclear Security Administration contractors. Contractors with the CRD incorporated into their contracts must demonstrate compliance by meeting defined performance outcomes. Contractor performance requirements will be defined in contractual language.

Contractors are expected to regularly assess and report their performance against these requirements, ensuring all safeguards and security obligations are met consistently and measurably throughout the contract period.

A violation of the provisions of this CRD relating to the safeguarding or security of restricted data, special nuclear material, or other classified information or matter, may result in a civil penalty pursuant to section 234B of the *Atomic Energy Act of 1954*, as amended (42 United States Code § 2282b). The procedures for the assessment of civil penalties are in Title 10 Code of Federal Regulations § 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations. Any site security plan approved by an Officially Designated Federal Security Authority has the force and effect of a DOE Order or Manual; therefore, it is enforceable under 10 CFR § 824.

ATTACHMENT 2, CHAPTER I
SAFEGUARDS AND SECURITY PROGRAM

This Attachment provides requirements associated with Department of Energy (DOE) Order (O) 470.7 and requirements applicable to contracts in which the associated Contractor Requirements Document (CRD; Attachment 1 to DOE O 470.7) is inserted.

1. SECURITY PLANNING. The contractor is required to establish and maintain a Safeguards and Security (S&S) program that prioritizes implementing risk-based planning activities, as approved by the Officially Designated Federal Security Authority (ODFSA). This approach includes developing ODFSA-approved site-specific security plans and analyses that address identified risks to DOE assets, personnel, and operations, and regularly assess and report performance.

   a. The purpose of this section is to establish the DOE's physical protection strategies for safeguarding Departmental assets.

   b. For the National Nuclear Security Administration (NNSA) and its subordinate offices, the design-basis threat (DBT), as defined in DOE O 470.3, serves as the baseline planning document. The DBT provides a starting point for analyzing potential threats against DOE assets.

   c. All other Departmental elements must tailor their physical protection strategies to site-specific conditions. Using threat results approved by the ODFSA, these organizations must develop:

      (1) Adversary characteristics, including numbers, capabilities, equipment, and tactics.

      (2) Analytical methods for risk assessment and reporting.

      (3) Risk acceptance thresholds consistent with mission and protection needs.

      (4) Risk reporting expectations and processes.

      (5) Defined risk acceptance authorities.

   d. Security Asset Categorization. DOE possesses assets that must be protected by S&S systems against site-specific threats based on the consequences of loss or sabotage with effects outside the distance established by the ODFSA. These assets include:

      (1) Special nuclear material (SNM).

      (2) Chemical and radiological material, nuclear material, and select agents and toxins.

      (3) Classified matter.

   e. Security Risk Acceptance. Contractors must use a vulnerability assessment or security risk assessment, as applicable, to analyze and communicate system effectiveness or overall security risk to DOE.

f. Graded Protection Concept. DOE must provide each site with the items listed in section c (1–5) based on site-specific threat results. The graded protection approach categorizes DOE assets.

g. Roll-Up of SNM. Roll-up must be considered when a defined threat has the capability to accumulate lower categories of SNM into greater quantities, thereby raising the total quantity to a higher SNM category. Accumulation occurs when the defined roll-up threat could move material to a single location and complete adversarial tasks. Site-specific threat results, material characterization, and associated analysis provide the basis for determining the credibility of roll-up. The ODFSA will approve the SNM configuration that requires a roll-up analysis and the scenarios, level of rigor, and documentation required for that analysis, and initiates consultation with the Material Risk Review Committee, if deemed necessary by the ODFSA, before making a decision.

2. INSIDER THREAT. Requirements applicable to the Insider Threat Program are contained in DOE O 470.5A, *Insider Threat Program*, current version.

3. PERFORMANCE ASSURANCE. Contractor will implement a performance assurance program as outlined in contractual language.

4. SAFEGUARDS AND SECURITY TRAINING PROGRAM. Contractor will establish an Officially Designated Security Authority (ODSA) approved training program that aligns with the knowledge, skills, and abilities based on appropriate job task analysis.

5. SAFEGUARDS AND SECURITY AWARENESS. Contractor will implement an S&S awareness program that provides briefings and supplemental awareness activities to all individuals to communicate personal security responsibilities. The program will:

   a. Ensure initial, periodic, and termination briefings are conducted as required for cleared individuals covering relevant security topics.

   b. Ensure that all individuals granted security clearances execute an SF 312, Classified Information Nondisclosure Agreement, prior to accessing classified information.

6. PROGRAM MANAGEMENT. The contractor will implement programs covering facility clearance (FCL), foreign ownership, control, or influence (FOCI) reviews, Departmental and foreign classified visits, and reporting of incidents of security concern (IOSCs).

7. RECORDS. Security-related records must be retained in accordance with the National Archives and Records Administration General Records Schedule (GRS) 5.6, Security Records, and DOE Administrative Records Schedule 18, Security, Emergency Planning, and Safety Records.

8. FACILITY CLEARANCES AND REGISTRATION AND FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE DETERMINATIONS. DOE contractors require an active FCL and favorable FOCI determination, and designation of a facility security officer when the contract or subcontract to be awarded is expected to require the officer to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter; SNM; 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. Contractor procedures applicable to the FOCI program must be documented in an ODFSA approved site security plan.

   a. If an FCL or FOCI determination is required, Contractors will submit information to DOE in accordance with 32 CFR § 117, National Industrial Security Program Operating Manual, 48 CFR § 904.70, Facility Clearance, 48 CFR § 952, Solicitation Provisions and Contract Clauses, and 10 U.S.C. § 4874(a–b), Award of certain contracts to entities controlled by a foreign government: prohibition.

   b. DOE granted FCLs based on a valid Department of Defense (DoD) FCL, Key management personnel (KMP) who do not need access to classified information are not required to obtain DOE access authorizations under 10 CFR § 710. Existing security clearances from another cognizant security agency fulfill KMP eligibility, with no duplicative DOE processing needed unless access to DOE-classified information is required.

9. CONTROL OF CLASSIFIED VISITS. The contractor will establish and maintain a classified visit program, if required, in accordance with t in 32 CFR § 117.16, Visits and Meetings. Procedures applicable to classified visits must be documented in ODFSA approved site security plans.

10. INCIDENTS OF SECURITY CONCERN.

   a. Requirements. An IOSC is an action or inaction contrary to S&S requirements because it poses a threat to national security or DOE security assets, including property, personnel, information, capabilities, or systems. IOSCs are categorized by significance type: infraction or violation. A violation is an event in which loss or compromise occurred or is suspected. An infraction is a procedural noncompliance that did not result in loss or compromise but could do so if left uncorrected. The ODSA must establish and administer an IOSC program using a graded approach based on event significance. The ODSA also develops and approves the criteria and methodology for local implementation. This program, criteria, and methodology must be documented in the ODFSA approved site security plan. The ODFSA must be notified of all violations and infractions involving unclassified controlled nuclear information and unclassified naval nuclear propulsion information.

b. Reporting. Initial and final reporting is imperative because the ODFSA has specific responsibilities for notifying and coordinating with other agencies, governments, Departmental leadership, and Congress for selected IOSCs. Reports of loss, compromise, or suspected compromise of classified information, whether foreign or domestic, must be reported to the cognizant security agency through the ODFSA in accordance with 32 CFR § 117.8.

11. NUCLEAR WEAPONS DATA/CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)/SIGMAS. The contractor will authorize and control the receipt, handling, and storage of nuclear weapons data, CNWDI, and Sigmas in accordance with DOE O 452.8.

12. UNCLASSIFIED FOREIGN NATIONAL ACCESS PROGRAM. Requirements applicable to unclassified foreign national access are contained in DOE O 142.3C.

13. PROTECTIVE FORCE OPERATIONS. The contractor will establish and maintain standardized requirements for managing, administering training programs, maintaining qualifications, and executing operations for various Protective Force (PF) activities. In addition, the contractor will implement a risk-based approach to establish posts and patrols, optimizing resource utilization. The contractor will:

a. Implement the requirements within 10 CFR §851, Worker Safety and Health Program; Appendix A to § 851, "Worker Safety and Health Functional Areas"; 10 CFR § 046, Medical, Physical Readiness, Training, and Access Authorization Standards for Protective Force Personnel; 10 CFR §1047, Limited Arrest Authority and Use of Force by Protective Force Officers; and 10 CFR §1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve, as applicable.

b. Management and Planning. Contractors must establish and operate PF programs that align with DOE requirements. This includes clearly identifying the protection mission, documenting resource needs, tracking personnel and equipment, and developing funding requirements.

(1) PF planning is based on threat guidance and adversary capabilities.

(2) Site-specific rules of engagement must be developed, incorporating the concept of hostile intent, considering protected assets, and establishing clear conditions for the use of deadly force, requiring approval from the ODFSA and local Office of General Counsel.

(3) Contractors must develop site-specific fresh pursuit procedures, approved by the ODFSA, that guide PF personnel in pursuing suspected criminals across jurisdictional lines, emphasizing safety and legal considerations.

(4) Contractors must develop formal officer-involved shooting procedures that provide clear guidance for PF personnel covering required actions, evidence preservation, reporting, and post-incident responsibilities. These procedures must be submitted to the ODFSA for approval.

(5) Contractors must implement approved work stoppage contingency plans that are approved by the ODFSA.

(6) Specialized functions (e.g., unmanned aerial systems or counter unmanned aerial systems operations) must conform to 10 U.S.C. § 6227, be based on identified risk, and be approved by the cognizant Program Secretarial Office.

(a) Contractors must ensure personnel are trained and programs are approved by the ODFSA.

a. Medical, Physical Readiness, and Training Requirements for PF Personnel. The contractor must establish and implement medical, physical readiness, and training requirements to ensure that PF personnel can respond within site-specific response times in accordance with applicable regulations including 10 CFR § 1046. These requirements should be based on a site-specific analysis approved by the ODSA and directed by the ODFSA. Security police officers and candidates must demonstrate general fitness measures related to their site and position, including muscular strength, muscular endurance, aerobic endurance, anaerobic endurance, agility, power, and mobility.

b. Duties. The contractor must establish and implement PF duties in accordance with applicable regulations, site-specific operational needs, and threat determinations.

c. Weapons and Munitions. The contractor must establish and implement PF weapons and munitions requirements in accordance with applicable regulations.

(1) Firearms Modifications. The ODSA must provide written approval for firearms modifications.

(2) Firearms and Munitions Handling and Storage. The ODSA must approve the storage of firearms, ammunition, pyrotechnics, and explosives.

(3) Firearms and Munitions Inventory. The ODSA will approve the conduct and documentation for inventory of:

(a) Firearms.

(b) Ammunition, pyrotechnics, and explosives.

(c) Firearms Safety. The contractor must establish and implement PF Firearms Safety requirements in accordance with applicable regulations.

a. Facilities and Equipment. The contractor will establish and implement PF facilities and equipment requirements in accordance with applicable DOE regulations and site-specific threat analysis results.

b. Performance Testing. The contractor must test or assess site-specific essential PF job functions as outlined in the ODFSA approved security plan.

14. PHYSICAL PROTECTION PROGRAM. The contractor must set and maintain performance standards for all physical protection activities, based on DOE or Program Office guidance and local threat assessments, and supported by ODFSA-approved security analysis. Measures should be risk-based, focusing resources on significant risks and tailoring systems to each asset's vulnerabilities to support the facility mission.

a. Physical Protection Planning. The contractor must develop local physical protection strategies, incorporating security systems, documented in the ODFSA-approved site security plan. All security strategies will be implemented in accordance with applicable federal regulations.

b. The following plans, programs, and strategies must be developed locally, based on local analysis and under the direction of the ODSA. They must be documented in an ODFSA-approved site security plan in accordance with 32 CFR 2001.41:

(1) Security locks and key program.

(2) Physical barriers for classified information, safeguards information, and SNM.

(3) Secure storage protection program.

(4) Vault construction and protection.

(5) Entry and exit screening plan.

(6) Physical protection strategies for classified information and controlled unclassified information (CUI).

(7) Physical protection strategies for assets.

(8) Emergency response plan for security areas.

(9) Protection measures for the transportation of SNM.

(10) SNM storage locations and PF post-construction requirements.

(11) Prohibited and controlled articles.

(12) Posting requirements that comply with applicable federal regulations.

c. Physical Protection Systems (PPS).

(1) The contractor must implement the design, protection measures, testing, and maintenance for PPS. This may include PPS networks, physical access-control systems, intrusion detection systems, video assessment and surveillance systems, plans, procedures, equipment, and strategies as documented in the ODFSA-approved site security plan.

(2) Special Access Program Facilities and Sensitive Compartmented Information Facilities must adhere to applicable federal policies.

15. VETTING.

a. Personnel Security. Requirements applicable to determining eligibility for access to classified information, including restricted data (RD) and SNM, are contained in *Atomic Energy Act of 1954*, as amended, EO 12968, EO 10865, EO 13467, 10 CFR §710, DOE O 472.2A, *Personnel Security* (current version), and various Office of the Director of National Intelligence directives.

b. Badging.

(1) The contractor will develop a site-specific Badge Program, utilizing a risk-based approach to determine credentialing and access requirements and will be documented in an ODFSA approved site security plan. The Badge Program must align with the applicable Homeland Security Presidential Directive 12 (HSPD-12) requirements that are outlined in DOE O 206.2, "Identity, Credential, and Access Management," and DOE O 472.2A, "Personnel Security."

(2) The program should assess the level of risk associated with various roles and access areas, ensuring that badging procedures and access permissions are tailored to mitigate identified risks and support operational security needs.

c. Human Reliability Program (HRP). Requirements applicable to HRP are contained in 10 CFR § 712, Human Reliability Program. The contractor must ensure that only the minimum number of individuals necessary for effective operations are enrolled in the HRP. The contractor shall periodically review the list of HRP position designations and enrolled individuals to ensure minimum number of participants for effective operations.

16. INFORMATION SECURITY. The contractor is responsible for establishing programs to safeguard and manage classified information and matter in accordance with applicable laws, regulations, EOs, government-wide policy directives and guidelines, as well as DOE policies and directives, which will be documented in an ODFSA-approved site security plan.

a. Classification Program. Requirements applicable to Classification Programs are contained in the *Atomic Energy Act* (RD, formerly restricted data [FRD], and transclassified foreign nuclear information [TFNI]), EO 13526 (National Security Information [NSI]), 10 CFR § 1045, 32 CFR § 2001, and DOE O 475.2B, *Identifying Classified Information*.

b. Classified Matter Protection and Control. Requirements applicable to marking, handling, protecting, storing, dispositioning, and destroying classified matter are contained in 32 CFR § 2001, 32 CFR § 117, and 10 CFR § 1045.

(1) The contractor will maintain a program that protects and controls classified matter based on federal requirements as implemented by ODFSA-approved security measures that result in protection, storage, or disposition effectiveness for classified matter.

(2) Processes and procedures related to the protection and control of classified matter will be documented in an ODFSA-approved security plans and procedures, reference documents, and training material.

c. Unclassified Controlled Nuclear Information. Requirements applicable to unclassified controlled nuclear information (UCNI) are contained in 10 CFR § 1017, Identification and Protection of Unclassified Controlled Nuclear Information. DOE federal and contractor employees must submit specific requests to deviate from the CFR to the Director, Office of Classification, for approval, in coordination with the Associate Administrator for Defense Nuclear Security for requests within NNSA.

(1) The ODFSA-approved site security plan must establish the process for designating UCNI reviewing officials and prescribe procedures to be followed when UCNI guidance is unclear or when no applicable guidance exists.

(2) Nomination. An employee nominated to be a Reviewing Official must be competent in the subject areas in which the authority will be used and familiar with DOE UCNI policy, procedures, and guidance.

(3) Headquarters. The immediate supervisor of an employee being nominated for Reviewing Official Authority must submit the required information identified in paragraph 16.c.(5), below, through the Headquarters Classification Representative.

(4) Field. The immediate supervisor of an employee being nominated for Reviewing Official authority must submit the information identified in paragraph 16.c(5) below to the Classification Officer or, if there is no Classification Officer, to the Director, Office of Classification, for DOE elements or to the Associate Administrator for Defense Nuclear Security for NNSA elements.

(5) Required Information.

(a) The employee’s name, organization, mailing address, telephone number, and e-mail address.

(b) Subject areas in which the authority will be used.

(c) Desired jurisdiction.

(d) Any special limitations on the authority.

(6) Training. The nominated employee must successfully complete the training for Reviewing Official Authority prior to appointment, which must include a practical examination using applicable UCNI guidance and applying UCNI markings. The required training and/or examination may be waived if the nominated employee has completed the training and/or examination within the last three years. However, the expiration date for the authority must be no longer than three years from the most recent successfully completed training.

(7) Appointment. The appointment must be in writing and must provide a description of the authority that includes the individual's name, organization, the effective date, the specific subject areas covered by the authority, the jurisdiction of the authority, the expiration date, and any special instructions or limitations on the authority. The appointing official must notify the employee and the employee's supervisor. At Headquarters, the appointing official must also notify the Headquarters Classification Representative.

(8) Authority Limitations. An employee may exercise his or her Reviewing Official authority only in the specific subject areas and jurisdiction covered in his or her authority description and in keeping with any special limitations imposed. The employee may not redelegate the authority. If an employee changes positions, the employee may retain the Reviewing Official authority with written approval of their new supervisor. The supervisor must then notify the appointing official of this action.

(9) Reappointment. If the authority is still needed after the initial three-year period, the employee must successfully complete an examination that retests his or her proficiency in using UCNI guidance and applying UCNI markings. If this examination is not successfully completed before the authority expires, the appointing official may grant a one-time three-month extension of the authority. If the examination is not successfully completed by the end of the three-month extension, the authority must be terminated.

(10) Cancellation of Authority. An employee's supervisor, the Classification Officer, or the appointing official may cancel this authority when an employee no longer requires such authority or if the employee does not exercise the authority reliability. Notification must be made to the employee and other parties identified above of the cancellation and effective date.

d. Controlled Unclassified Information. Requirements applicable to CUI are contained in 32 CFR § 2002, Controlled Unclassified Information (CUI).

e. Operations Security. Develop Operations Security plans at the direction of the ODSA and document them in local procedures to integrate with applicable programs to protect identified critical program information as set forth in the National Security Presidential Memorandum-28. Threat analysis will be documented in the ODFSA approved site security plan.

17. TECHNICAL SECURITY. Requirements applicable to the Technical Security Program are contained in DOE O 470.6, *Technical Security Program*, current version.

18. NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY (MC&A). Contractors must establish an ODFSA approved graded MC&A program for controlling, accounting for, and safeguarding SNM and other accountable nuclear material.

f. The Nuclear Materials Management and Safeguards System User Guide is used for nuclear materials management and Safeguards System reporting and data submission.

g. For DOE to Department of War (DoW) weapons transfers, SNM in weapons must not be transferred to DoW under 42 U.S.C. § 2121(b), "Material for Department of Defense Use," until DOE has received direction from the President.

h. Program Management. The contractor will develop a detailed ODFSA approved MC&A Plan that outlines specific roles, responsibilities, training, and procedures to promote clarity and accountability. The program should document control measures and program elements, be graded based on potential loss consequences, monitor effectiveness and respond to loss indicators, and integrate with S&S programs. This structured approach reduces confusion and ensures that all personnel are aware of their duties, leading to more efficient operations.

i. Material Accounting. Each facility will have a system that tracks SNM inventories, documenting SNM transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and SNM gains or losses. Each facility must have an accountability system that provides continuity of knowledge for SNM from receipt or production to disposition and include access authorization to the accountability system. Each facility must be able to produce an inventory of all nuclear material in the accountability system upon request. The accountability system will be maintained and updated in a timely manner, as approved by the MC&A Plan. Material Balance Areas (MBAs) shall be used to identify the location and quantity of SNM and collocate credible substitution material in the facility. An MBA is an area that is both a subsidiary account of material within the accounting system at a facility and a specified geographical area that has defined boundaries.

j. Material Control. Contractors must implement a Material Control Program consistent with the graded safeguards concept to prevent unauthorized removal of SNM.

(1) Ensure each facility implements a Material Control Program concept to ensure that SNM is not removed from an authorized location without approval or timely detection of an unauthorized removal.

(a) This includes access controls, material surveillance, material containment, detection and assessment, portal monitoring, and incident reporting and response.

k. Measurements. Ensure all facilities possessing SNM implement Measurements and Measurement Control programs. The Measurements program must provide measured values with uncertainties sufficient to detect theft or diversion of SNM. The Measurement Control program must ensure the quality of measurements made for MC&A purposes. The Measurement program elements include measurement types, methods, control, and bulk sampling. Measurements are required as directed in the MC&A Plan. Category IV sites, where roll-up to Category III has been deemed not-credible and items are not susceptible to theft or diversion, as determined by a vulnerability assessment, may be excluded from the requirements of section 1(g).

l. Physical Inventory. A physical inventory program for SNM must be implemented to confirm materials are in their stated quantities and authorized locations, and to detect unauthorized removals or discrepancies. The Physical Inventory Program:

(1) Will be conducted at a frequency approved by the ODFSA.

(2) Outlines procedures for conducting, verifying, and reconciling inventories.

(3) Ensures that discrepancies between the physical inventory and the accounting records system are detected and resolved.

(4) Include periodic physical inventories, special inventories, and International Atomic Energy Agency inventories (if applicable)

(5) The risk associated with substitution material should be considered in the facility Physical Inventory Plan.

Table 1. Special nuclear materials.

Material Type	Accountable Quantity	Weight Field Used for Element	Weight Field Used for Isotope	Material Type Code
Enriched Uranium (U-235)	1 gram	Total U	U-235	20
Uranium-233[3]	1 gram	Total U	U-233	70
Plutonium-242[1] (Pu)	1 gram	Total Pu	Pu-242	40
Plutonium-239–241	1 gram	Total Pu	Pu-239 + Pu-241	50

Material Type	Accountable Quantity	Weight Field Used for Element	Weight Field Used for Isotope	Material Type Code
Plutonium-238[2]	1/10 of a gram	Total Pu	Pu-238	83
Uranium in cascades	1 gram	Total U	U-235	89

[1] Account as Pu-242 (MT 40) if the contained Pu-242 is 20% or greater of total plutonium by weight; otherwise, account as Pu-239-241 (MT 50).
[2] Account as Pu-238 (MT 83) if the contained Pu-238 is 10% or greater of total plutonium by weight; otherwise, account as Pu-239-241 (MT 50).
[3] Account as U-233 (MT 70) if the contained U-233 is 10% or greater of total uranium by weight; otherwise, account as U235 (MT 10, 20, or 81).
When separated, Am and Np must be controlled and accounted for as required by Attachment 2, Chapter I of this Order.

Table 2. Controlled and accounted for as SNM

Material Type	Accountable Quantity	Weight Field Used for Element	Weight Field Used for Isotope	Material Type Code
Americium-241**(Am)	1 gram	Total Am	Am-241	44
Americium-243**	1 gram	Total Am	Am-243	45
Neptunium-237** (Np)	1 gram	Total Np	-	82

** Americium and Np-237 contained in SNM are not required to be accounted for until separated. If separated, these materials must be controlled and accounted for as SNM.

Table 3. Graded safeguards

Graded Safeguards Table									
Material Types	Attractiveness Level[3]	Pu/U-233[2] Category (kg)				Contained U- 235/Separated Np-237/Separated Am-241 and Am-243 Category (kg)			
		I	II	III	IV[1]	I	II	III	IV[1]
WEAPONS Assembled weapons and test devices	A	All	N/A	N/A	N/A	All	N/A	N/A	N/A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B	≥2	≥0.4 <2	≥0.2 <0.4	<0.2	≥5	≥1<5	≥0.4 <1	<0.4
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF_4 or UF_6 (≥50% enriched)	C	≥6	≥2<6	≥0.4 <2	<0.4	≥20	≥6 <20	≥2 <6	<2

Graded Safeguards Table									
Material Types	Attractiveness Level[3]	Pu/U-233[2] Category (kg)				Contained U- 235/Separated Np-237/Separated Am-241 and Am-243 Category (kg)			
		I	II	III	IV[1]	I	II	III	IV[1]
LOW-GRADE MATERIALS UF_4 or UF_6 (≥20% and <50% enriched); Solutions (1– 25 g/L); process residues requiring extensive reprocessing; Pu-238 (except waste)	D	N/A	≥16	≥3 <16	<3	N/A	≥50	≥8 <50	<8
ALL OTHER MATERIALS Highly irradiated forms, solutions (<1 g/L), compounds; uranium containing <20% U-235 or <10% U-233(any form, any quantity)	E	N/A	N/A	N/A	Reportable Quantities	N/A	N/A	N/A	Reportable Quantities

1 The lower limit for Category IV is equal to reportable quantities in this Order.
2 In items that contain U-233 and U-235, if the contained U-233 is 10% or greater of total uranium by weight, then the effective quantity of U-233 = (contained U-233 + contained U-235). The category is then determined by using the effective quantity of U-233 compared with the Pu/U-233 side of the table.
3 Attractiveness level descriptions are examples only and not all inclusive. Additional examples appropriate to a given site should be included in the Nuclear Material Control and Accountability plan.
4 Directions for determining the material category when multiple material types and attractiveness levels are being considered can be found in DOE-STD-1194.

Table 4. Factors for calculating effective quantities

Attractiveness Level	Pu/U-233 Factor	Contained U-235/Separated Np-237/Separated Am-241 and Am-243 Factor
B	1	1
C	1/3	1/4