

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 457.1B

Approved: 08-05-2026

SUBJECT: NUCLEAR COUNTERTERRORISM

1. PURPOSE. This Order establishes Departmental requirements to reduce the risk of inadvertent or unauthorized disclosure of sensitive improvised nuclear device (IND) information by:
 - a. Requiring identification and protection of sensitive IND information;
 - b. Establishing Departmental responsibilities for identifying and protecting sensitive IND information;
 - c. Establishing controls on dissemination of sensitive IND information, including use of the Sigma 20 nuclear weapon data (NWD) control category; and
 - d. Defining appropriate means for providing IND-related information at an appropriate level of classification to other federal agencies to support national security objectives.

This Order supports implementation of applicable national policy and strategy for protecting the homeland against nuclear terrorism.

2. CANCELS/SUPERSEDES. Department of Energy (DOE) Order (O) 457.1A, *Nuclear Counterterrorism*, dated August 26, 2013.

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contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.
 - a. Departmental Applicability. Except for the equivalencies/exemptions in Paragraph c of this section, this Order applies to all Departmental Elements.

- b. National Nuclear Security Administration (NNSA) Applicability. The Administrator of the NNSA must ensure that NNSA employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order must be construed to interfere with the NNSA Administrator's authority under Section 3212(d) of Public Law 106-65, National Defense Authorization Act for Fiscal Year 2000, to establish Administration-specific policies, unless disapproved by the Secretary.
- c. 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, including as amended or updated.
- d. Equivalencies/Exemptions.
 - (1) Naval Nuclear Propulsion Program Equivalency. In accordance with Executive Order 12344, The Naval Nuclear Propulsion Program, codified at 50 U.S.C. §§ 2406, Deputy Administrator for Naval Reactors, and 2511, and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) must implement and oversee requirements and practices pertaining to this Order for activities under the Director's cognizance, as deemed appropriate.
- e. Exemptions.
 - (1) Organizations prohibited from accessing sensitive IND information.
 - (2) Requests for exemptions are jointly approved by Program Secretarial Officers and the Associate Administrator for Counterterrorism and Counterproliferation, with conflicts resolved by the Deputy Secretary or designated Departmental Chief Operating Officer.
 - (3) Requests for exemptions must be submitted from the Cognizant Field Element Manager to the appropriate Program Secretarial Officer(s) and the Associate Administrator for Counterterrorism and Counterproliferation.

4. REQUIREMENTS.

- a. Sensitive IND information must be identified and protected to preclude terrorists and other unauthorized persons from obtaining and exploiting it.
- b. Sigma 20, an NWD control category, must be used to restrict the dissemination of sensitive IND information in the interest of national security.
- c. This Order provides the basis for implementing procedures regulating strict control of and access to Sigma 20 NWD, and all holders of that information must comply with this Order.
- d. IND design-related work shall be conducted only at those locations in the DOE complex designated by the Director, Office of Nuclear Threat Science.

5. RESPONSIBILITIES.

- a. Deputy Under Secretary for Counterterrorism and Counterproliferation/Associate Administrator for Counterterrorism and Counterproliferation.
 - (1) Provide Departmental guidance for nuclear counterterrorism activities, including IND information control policy within DOE/NNSA and with other federal agencies.
 - (2) Authorize and oversee IND design-related work.
 - (3) Manage DOE/NNSA oversight of IND information control.
 - (4) Direct nuclear design-related research and development activities to ensure weapons physics, engineering, analysis, information, and nuclear weapons technologies are applied adequately, effectively, and correctly to address IND-related issues.
- b. Director, Office of Nuclear Threat Science.
 - (1) Implement all aspects of IND information control as defined in this Order, including administration of the Sigma 20 category of NWD.
 - (2) Designate locations within the DOE complex where IND design-related work may be performed.
 - (3) In coordination with the Heads of Field Elements, notify contracting officers when DOE contractors are affected by this Order.
 - (4) Perform annual program reviews to evaluate ongoing activities; future plans and projects; resource requirements, including the resources necessary to implement and administer this Order; and major concerns and issues.

- (5) Ensure all Strategic Partnership projects at the national laboratories that use IND design information are reviewed, approved, and comply with this directive.
 - (6) Recommend to the Associate Administrator for Counterterrorism and Counterproliferation revisions to Sigma 20 implementation, as necessary.
 - (7) Develop agreements with federal agencies and implement security procedures as required for handling Sigma 20 NWD.
 - (8) Deputy Administrator for Defense Nuclear Nonproliferation. Coordinates any IND-related work with the Associate Administrator for Counterterrorism and Counterproliferation to fulfill the requirements for Sigma 20 NWD.
- c. Associate Administrator for Emergency Operations.
 - (1) Responsible, during a radiological asset response operation, for the security and control of Sigma 20 NWD of any form.
 - (2) Coordinate all IND-related work with the Associate Administrator for Counterterrorism and Counterproliferation to fulfill the requirements for Sigma 20 NWD.
- d. Director, Office of Intelligence and Counterintelligence.
 - (1) Serve as the lead proponent for IND information control within the Intelligence Community on behalf of DOE/NNSA.
 - (2) Provide intelligence-related information concerning nuclear terrorism to the Associate Administrator for Counterterrorism.
 - (3) Conduct counterintelligence (CI) activities, including Counterintelligence Evaluation Program, to protect DOE/NNSA information, personnel, and assets from international terrorist activities and from intelligence collection by or on behalf of foreign powers or entities.
 - (4) Ensures all IND design-related intelligence work projects at the national laboratories comply with this directive and coordinates all IND design-related intelligence work projects with the Office of Nuclear Threat Science.
- e. Deputy Administrator for Defense Programs.
 - (1) Support the activities of the Counter Terrorism/Counter Proliferation programs at the NNSA laboratories and plants, as necessary.

- (2) Oversees Strategic Partnership Projects at the national laboratories in accordance with DOE O 481.1D, *Strategic Partnership Projects*, with applicable guidance, and
 - (3) Coordinate all potential IND-related projects with the Office of Nuclear Threat Science. These may include:
 - (a) Use Control projects with IND implications.
 - (b) United States (U.S.) nuclear weapons that have been adversary-modified.
 - (c) Projects related to portions or components of U.S. nuclear weapons that may be used in INDs.
 - f. Associate Administrator for Security Operations (NA-70). Responsible for the overall direction and management of physical, personnel, technical, materials control and accounting, and classified and sensitive information security programs at NNSA facilities.
 - g. Heads of Field Organizations.¹
 - (1) Verify the appropriate field locations and facilities are operated in compliance with security procedures established for IND information control.
 - (2) In coordination with the Director, Office of Nuclear Threat Science, notify contracting officers when DOE contractors are affected by this Order.
 - (3) Notify the Director, Office of Nuclear Threat Science of any IND-related work-for-others project not processed through DOE-IN.
 - h. Contracting Officers. 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. Note: DOE O 251.1, *Departmental Directives Program*, current version, provides a definition for “invoked technical standard.”

¹ Operations offices, service centers, site offices, area offices, field offices, project management offices, and regional offices of federally staffed laboratories

7. DEFINITIONS.

- a. Improvised Nuclear Device. A device, including adversary-modified U.S. or foreign nuclear weapons, incorporating nuclear (actinide) materials, that is designed, constructed, or modified outside of an official government agency and which has, appears to have, or is claimed to have the capability to produce a nuclear explosion. (See DOE CG-IND-2, DOE Classification Guide for Improvised Nuclear Devices, or its successor for details.)
- b. Nuclear Weapon Data. Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear explosives, nuclear weapons, or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. NWD is matter in any combination of documents or material, regardless of physical form or characteristics.
- c. Sigma 20 NWD. A specific category of NWD pertaining to “crude, simple, or innovative” IND designs, concepts, and related manufacturing or processing pathways. Not all INDs are covered under the Sigma 20 category (see DOE CG-IND for further details).

8. REFERENCES.

- a. Public Law (P.L.) 83-703, The Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, Congressional declaration of policy), which governs civilian and military uses of nuclear materials and facilities.
- b. Title XXXII of P.L. 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within the DOE.
- c. “National Strategy to Combat Weapons of Mass Destruction,” dated December 2002, which specified all needed capabilities to combat weapons of mass destruction (WMD) be fully integrated.
- d. “National Strategy for Counterterrorism,” dated June 2011, which articulates the U.S. government’s approach to countering terrorism and identifies the range of tools used.
- e. “The National Strategy for Homeland Security,” dated October 2007, Office of Homeland Security, which provides policy guidance for securing the U.S. homeland from terrorist attacks.
- f. National Security Presidential Directive 28, “United States Nuclear Weapons Command and Control, Safety, and Security (U),” dated June 20, 2003 (Secret), which provides the basis for the maintenance of a nuclear command and control system under the authority and direction of the Commander in Chief, and establishes nuclear surety policy.

- g. 10 CFR § 709, Counterintelligence Evaluation Program, dated September 29, 2006, which outlines the DOE polygraph examination program.
- h. DOE O 153.1A, *Departmental Nuclear Emergency Support Team Capabilities*, dated October 28, 2022, which establishes requirements and responsibilities for the DOE/NNSA national radiological emergency response assets and capabilities and Nuclear Emergency Support Team assets.
- i. DOE O 200.1A Chg 2, *Information Technology Management Program*, dated August 11, 2023, and National Archives and Record Administration-approved DOE records schedules, which describe requirements for managing records related to this program.
- j. DOE P 411.2C, *Scientific and Technical Information Management*, dated July 24, 2025, which ensures that this information is appropriately managed as part of the DOE mission to enable the advancement of scientific knowledge and technological innovation.
- k. DOE O 470.1A, *Safeguards and Security Program Operations Management*, dated December 18, 2024, which addresses facility clearances, foreign ownership and control determinations, classified visits and information of security concerns.
- l. DOE O 470.4C, *Safeguards and Security Planning*, dated December 23, 2024, which establishes safeguards and security planning for protection of materials and DOE facilities.
- m. DOE O 470.3C, Chg 2, “Design Basis Threat,” dated February 23, 2024, which establishes threat metrics for the protection of nuclear weapons, nuclear weapons components, special nuclear materials, national laboratories, plants and other critical Departmental assets.
- n. DOE O 471.6 Chg 4, “Information Security,” dated August 22, 2023, which establishes security requirements for the protection and control of information and matter required to be classified or controlled by statutes, regulations, or DOE directives.
- o. DOE O 472.2A, *Personnel Security*, dated October 28, 2024, which establishes the overall objectives and requirements for the Department of Energy Personnel Security Program.
- p. DOE O 473.3, *Protection Program Operations*, dated June 29, 2011, which establishes the requirements for protection of facilities, buildings, and government property, including classified information, special nuclear materials, and nuclear weapons.
- q. DOE O 475.1, *Counterintelligence Program*, dated December 10, 2004, which establishes CI Program requirements and responsibilities for the Department of Energy, including the NNSA.

08-05-2026

- r. DOE O 481.1D, *Strategic Partnership Projects* (formerly known as *Work for Others [Non-Department of Energy Funded Work]*), dated December 5, 2016, for work for non-DOE entities by DOE/NNSA and/or their respective contractor personnel or the use of DOE/NNSA facilities not funded by DOE appropriations.
 - s. DOE O 484.1 Chg 4, “Reimbursable Work for the Department of Homeland Security,” dated October 28, 2024, which establishes DOE policies and procedures for reimbursable work funded by the Department of Homeland Security.
 - t. CG-IND-2 Chg 2, “DOE Classification Guide for Improvised Nuclear Devices,” dated May 2025.
9. CONTACT. For assistance regarding this directive, contact the Director, Office of Nuclear Threat Science, (202) 586-4582.

BY ORDER OF THE SECRETARY OF ENERGY:



JAMES P. DANLY
Deputy Secretary