

SUBJECT: NUCLEAR COUNTERTERRORISM

1. **OBJECTIVES.**

- a. To support Department of Energy (DOE) activities for public health, safety, and common defense by reducing the threat of inadvertent or unauthorized disclosure of sensitive improvised nuclear device (IND) information.
- b. To support the implementation of high-level policy guidance for protecting the homeland against nuclear terrorism as outlined in the National Strategy for Combating Terrorism and the National Strategy for Homeland Security.
- c. To establish DOE responsibilities for identifying and protecting sensitive IND information.
- d. To establish controls on the dissemination of sensitive IND information.
- e. To define appropriate means for providing IND-related information at an appropriate level of classification to other Federal agencies to assist in meeting national security objectives.

2. **CANCELLATION.** None.

3. **APPLICABILITY.**

- a. **All Departmental Elements.** Except for the exclusions in paragraph 3c, this Order applies to all departmental elements. Attachment 1 is a complete listing of DOE organizations to which this Order is applicable and organizations that are prohibited from accessing sensitive IND information without specific approval from the Assistant Deputy Administrator for Military Application and Stockpile Operations.

The National Nuclear Security Administration (NNSA) Administrator will assure that NNSA employees and contractors comply with their respective responsibilities under this Order.

- b. **DOE Contractors.** Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to DOE contracts that include the CRD.
- c. **Exclusions.** This Order does not apply to activities conducted under the authority of the Director, Naval Nuclear Propulsion Program, as assigned by Executive Order 12344.

4. REQUIREMENTS.

- a. Identify sensitive IND information and implement appropriate measures to preclude terrorists/unauthorized persons from obtaining and exploiting it.
- b. Establish Sigma 20 as a nuclear weapon data (NWD) control category to restrict the dissemination of sensitive IND information in the interest of national security.
- c. Provide the basis for implementing procedures regulating strict control of and access to Sigma 20 NWD.
- d. Prohibit the performance of IND design-related work from being conducted at any location in the DOE complex unless authorized by the Assistant Deputy Administrator for Military Application and Stockpile Operations.
- e. Develop agreements with Federal agencies and implement security procedures as required for handling Sigma 20 NWD.

5. RESPONSIBILITIES.

- a. Deputy Under Secretary for Counterterrorism. Provides guidance on Department activities related to nuclear counterterrorism, including IND information control policy within DOE/NNSA and other Federal agencies.
- b. Deputy Administrator for Defense Programs.
 - (1) Oversees all IND design-related work.
 - (2) Manages DOE/NNSA oversight of IND information.
 - (3) Establishes a new NWD category called Sigma 20 to control access to and dissemination of IND information.
 - (4) Directs nuclear design-related research and development activities so that the full range of weapons physics knowledge, engineering, analysis, information, and nuclear weapons technologies are applied adequately and correctly to provide the best possible technical solutions to IND-related issues.
- c. Assistant Deputy Administrator for Military Application and Stockpile Operations.
 - (1) Implements all aspects of IND information control as defined in this Order, including administration of the Sigma 20 category.

- (2) Designates locations within the DOE complex where IND design-related work may be performed.
 - (3) Notifies contracting officers when DOE contractors are affected by this Order.
 - (4) Performs 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) Recommends to the Deputy Administrator for Defense Programs revisions to Sigma 20 implementation, as necessary.
- d. Deputy Administrator for Defense Nuclear Nonproliferation. Coordinates all IND-related work with the Deputy Administrator for Defense Programs to fulfill the requirements for Sigma 20 NWD.
- e. 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) Coordinates all IND-related work with the Deputy Administrator for Defense Programs to fulfill the requirements for Sigma 20 NWD.
- f. Director, Office of Intelligence.
 - (1) Serves as the lead proponent for IND information control within the Intelligence Community on behalf of DOE/NNSA.
 - (2) Provides intelligence-related information concerning nuclear terrorism to the Deputy Under Secretary for Counterterrorism.
- g. Chief, Office of Defense Nuclear Counterintelligence. Conducts counterintelligence (CI) activities 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.
- h. Associate Administrator for Defense Nuclear Security. 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.
- i. Director, Office of Independent Oversight. Through the Director, Office of Security Evaluations, provides independent inspections and evaluations to assess physical security, and classified matter protection and control effectiveness.

- j. Heads of Field Organizations.¹ Verify that their field locations and facilities are operated in compliance with security procedures established for IND information control.
 - k. Contracting Officers. After being notified, incorporate the DOE O 457.1 CRD into affected contracts via the laws, regulations, and DOE directives clause of the contracts.
6. DEFINITIONS. See Attachment 3.
7. REFERENCES.
- a. Public Law (P.L.) 83-703, the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011), 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 Department of Energy.
 - c. National Strategy for Combating Terrorism, dated February 2003, in which the President of the United States describes the nature of the terrorist threat, details U.S. strategic intent, and provides goals and objectives for the campaign against terrorism.
 - d. The National Strategy for Homeland Security, dated July 2002, Office of Homeland Security, provides policy guidance for securing the U.S. homeland from terrorist attacks.
 - e. National Security Presidential Directive 28, United States Nuclear Weapons Command and Control, Safety, and Security (U), dated 6-20-03 (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.
 - f. DOE O 200.1, *Information Management Program*, dated 9-30-96, and National Archives and Record Administration-approved DOE records schedules, which describe requirements for managing records related to this program.
- DOE O 470.3, *Design Basis Threat Policy* (U), dated 10-10-04 (Secret), which describes DOE security objectives, policies, and prescribes the "threat-based" security metrics for the protection of nuclear weapons, nuclear weapons components, special nuclear material, national laboratories, plants, and other critical Departmental assets.

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

- g. DOE O 470.4, *Safeguards and Security Awareness Program*, dated 8-26-05, which establishes the roles and responsibilities for the U.S. Department of Energy Safeguards and Security Program.
 - h. DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, dated 8-26-05, which establishes program planning and management requirements for the Department's Safeguards and Security Program.
 - i. DOE M 470.4-2, *Physical Protection*, dated 8-26-05, which establishes requirements for the physical protection of safeguards and security interests.
 - j. DOE M 470.4-4, *Information Security*, dated 8-26-05, which establishes security requirements for the protection and control of information and matter required to be classified or controlled by statutes, regulations, or Department of Energy directives.
 - k. DOE M 470.4-5, *Personnel Security*, dated 8-26-05, which establishes the overall objectives and requirements for the Department of Energy Personnel Security Program.
 - l. DOE O 475.1, *Counterintelligence Program*, dated 12-10-04, which establishes CI Program requirements and responsibilities for the Department of Energy, including the National Nuclear Security Administration.
 - m. DOE O 5530.1A, *Accident Response Group*, dated 9-20-91, which establishes DOE policy for response to accidents and significant incidents involving nuclear weapons and/or components.
 - n. DOE O 5530.2, *Nuclear Emergency Search Team*, dated 9-20-91, which establishes DOE policy for Nuclear Emergency Search Team operations in response to malevolent radiological incidents.
8. CONTACT. Office of Nuclear Weapon Surety and Quality, 202-586-4582.

BY ORDER OF THE SECRETARY OF ENERGY:



CLAY SELL
Deputy Secretary

DOE ELEMENTS TO WHICH DOE O 457.1 IS APPLICABLE

Office of the Secretary

Departmental Representative to the Defense Nuclear Facilities Safety Board*

National Nuclear Security Administration

- Office of the Administrator
- Office of Counterterrorism
- Office of Congressional, Intergovernmental, and Public Affairs*
- Office of Defense Nuclear Counterintelligence
- Office of Defense Nuclear Nonproliferation
- Office of Defense Nuclear Security
- Office of Defense Programs
- Office of Emergency Operations
- Office of Environment, Safety and Health*
- Office of General Counsel
- Office of Infrastructure and Environment*
- Office of Management and Administration*
- Office of Policy Planning, Assessment, and Analysis

Office of the Chief Financial Officer*

Office of the Chief Information Officer*

Office of Congressional and Intergovernmental Affairs*

Office of Counterintelligence

Office of General Counsel

Office of Human Capital Management*

Office of the Inspector General

Office of Intelligence

Office of Nuclear Energy, Science and Technology*

Office of Policy and International Affairs*

Office of Science*

Office of Security and Safety Performance Assurance*

Office of Civilian Radioactive Waste Management*

Office of Economic Impact and Diversity*

Office of Electricity Delivery and Energy Reliability*

Office of Energy Efficiency and Renewable Energy*

Energy Information Administration*

* Except as approved by the Assistant Deputy Administrator for Military Application and Stockpile Operations, access to Sigma 20 information is prohibited for personnel within these organizations.

Office of Environment, Safety and Health*
Office of Environmental Management*
Office of Fossil Energy*
Office of Hearings and Appeals*
Office of Legacy Management*
Office of Management*
Office of Public Affairs*
Secretary of Energy Advisory Board*
Bonneville Power Administration*
Southeastern Power Administration*
Southwestern Power Administration*
Western Area Power Administration*

NOTE: Field entities should not to be listed unless there are special circumstances necessitating their inclusion.
Applicability to a Field entity is assumed when its Lead Program Secretarial Officer organization is listed.

* Except as approved by the Assistant Deputy Administrator for Military Application and Stockpile Operations, access to Sigma 20 information is prohibited for personnel within these organizations.

**CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 457.1, *NUCLEAR COUNTERTERRORISM***

1. Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this Contractor Requirements Document (CRD) and flowing down CRD requirements to subcontractors at any tier to the extent necessary to ensure contractor compliance.
2. This CRD establishes the requirements for Department of Energy (DOE) contractors whose contracts involve or could potentially involve accessing or generating nuclear weapon design information.
3. Contractors are required to protect IND information. To this end, contractors will implement a Sigma 20 nuclear weapon data (NWD) control category to control the dissemination of sensitive IND information in the interest of U.S. national security. Procedures will be implemented to provide for strict control of and access to Sigma 20 NWD. IND design-related work is not to be conducted at any DOE location unless authorized by the Assistant Deputy Administrator for Military Application and Stockpile Operations. In this context, IND design-related work includes generating:
 - any complete design of an IND, including speculative exploration of novel design concepts;
 - validation of comparative assessments of IND design alternatives;
 - descriptions of design and fabrication procedures likely to be employed by terrorists, including modeling or design methodologies, energetic or nuclear material specifications, component specifications (e.g., arming and firing system design), or other fabrication procedures; and
 - realistic IND designs to assess the performance of radiation detection systems, diagnostic equipment, security standards, and/or render-safe tools and procedures.
4. Contractors must support annual program reviews, when and as directed by the Assistant Deputy Administrator for Military Application and Stockpile Operations, to evaluate relevant ongoing activities; future plans and projects; resource requirements, including the resources necessary to implement and administer this Order; and major concerns and issues.
5. Contractors must maintain records according to National Archives and Records Administration-approved DOE or site-specific records retention schedules.

DEFINITIONS

1. Improvised nuclear device— a device, incorporating fissile materials, designed or constructed 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 CG-RER-1, DOE Classification and UCNI Guide for Radiological Emergency Response (U) for details.)
2. 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 weapons or nuclear weapon components, including information related to improvised nuclear devices.
3. Sigma 20—a specific category of nuclear weapon data that pertains to sensitive improvised nuclear device information.