Department of Energy
National Nuclear Security Administration
Washington, DC 20585

JM CHRONOLOGY
JM RECEIVED 1/11/13
OUT FOR REVIEW 2/1/13
DRB DISCUSSION 2/7/13

MEMORANDUM FOR: CYNTHIA A. LERSTEN
ASSOCIATE ADMINISTRATOR FOR
MANAGEMENT AND BUDGET

THROUGH: INGRID KOLB
DIRECTOR, OFFICE OF MANAGEMENT

FROM: STEVEN AOKI
ASSOCIATE ADMINISTRATOR FOR
COUNTERTERRORISM AND COUNTERPROLIFERATION

SUBJECT: Notice of Intent to Revise DOE Order on Nuclear Counterterrorism and cancel Manual on Control of Improvised Nuclear Device Information (currently DOE O 457.1 and DOE M 457.1-1 respectively).

PURPOSE: The purpose of the proposed directive is to replace the information contained in DOE O 457.1, "Nuclear Counterterrorism," approved February 7, 2006, and DOE M 457.1-1, Manual on Control of Improvised Nuclear Device Information, approved August 10, 2006, by revising the former and including the contents of the latter as appendices to the new DOE directive.

JUSTIFICATION: The revised DOE Order would consolidate and update existing departmental directives to include the content of a recent Secretarial decision memorandum.[1] This new combined directive would clarify internal roles and responsibilities, which have changed substantially within NNSA, and policy to protect classified information pertaining to sensitive Improvised Nuclear Weapon (IND) designs.

This Order would apply to all DOE offices and organizations that participate in matters pertaining to nuclear counterterrorism and counterproliferation, with a focus on classified IND matters. DOE/NNSA personnel have handled and protected sensitive IND design information using the Sigma 20 caveat since the current directives were approved in 2006.

---

[1] Edward Bruce Held (Director, Office of Intelligence and Counterintelligence) memorandum to Secretary, *"ACTION: to obtain the Secretary's approval to designate Sigma 20 personnel as subject to mandatory counterintelligence evaluations"*, April 11, 2012, approved by Steven Chu April 23, 2012.

ltr 1/11/2013 - cBelan

Beyond organizational changes, this revision includes a change to the application of the Counterintelligence Evaluation Program for personnel granted access to this sensitive classified information. The other substantial change requires that interagency efforts at DOE/NNSA facilities funded outside DOE/NNSA (previously termed "Work for Others") but relevant to sensitive IND design information be coordinated through the office of primary responsibility for protecting this information. Rather than publishing another separate Official Use Only (OUO) Order for details about how sensitive IND design information is handled and protected, that specific information would be included in OUO appendices.

There are no valid external, consensus, or other "Standards" (e.g., International Organization for Standardization (ISO), Voluntary Protection Programs (VPP)) available that can be used in place of this directive.

Upon issuance of this Order, request cancellation of DOE O 457.1, "Nuclear Counterterrorism," approved February 7, 2006, and DOE M 457.1-1, Manual on Control of Improvised Nuclear Device Information, approved August 10, 2006.

IMPACT: The proposed directive does not duplicate existing laws, regulations or national standards and it does not create undue burden on the Department. Because it does not create new requirements, this Order does not adversely impact any people across the department, within NNSA, or within the Office of Nuclear Threat Science (NA-82). Although fulfilling ongoing requirements for this directive necessitates the time of several Full-Time Equivalent (FTE) staff, no additional time should be required to implement this directive. Similarly, no new costs are anticipated, but costs would continue to include ongoing technical work budgeted and paid in support of the Office of Nuclear Threat Science (NA-82).

WRITER: Randall Weidman, Senior Policy and Plans Advisor, Office of the Associate Administrator for Counterterrorism and Counterproliferation, 202-586-7137.

OPI/OPI CONTACT: Jackson Q. Crocker, Acting Director, Office of Nuclear Threat Science, 202-586-4582.

Ingrid Kolb, Director, Office of Management (MA-1):

Concur: _____ Nonconcur: _____ Date: 2-7-2013

Cynthia A. Lersten, Associated Administrator for Management and Budget (NA-MB-1):

Concur: _____ Nonconcur: _____ Date: 2-8-13

Risk Identification and Assessment

Nuclear Counterterrorism

Risk	Probability	Impact	Risk Level
People			
1. Risk to personnel from terrorist acts of nuclear sabotage	Unlikely	High	Significant
Mission			
2. Inability to secure improvised nuclear device and related information.	Unlikely	High	Significant
3. Inability to stop terrorist nuclear device from functioning	Unlikely	High	Significant
Assets			
4. Risk to assets from terrorist acts of nuclear sabotage	Unlikely	High	Significant
Financial			
5. Cost of decommissioning, decontaminating, or rebuilding facilities, infrastructure, and/or cities following acts of nuclear terrorism	Unlikely	High	Significant
Customer and Public Trust			
6. Risk to US citizens and USG interests from acts of nuclear terrorism	Unlikely	High	Significant

Gap Analysis of Existing Risks and Controls

[Identify all controls that currently exist, excluding controls developed within this subsystem. Add more categories as necessary.]

Laws	• 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 • 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
External Regulation	• 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 • 10 CFR 709, *Counterintelligence Evaluation Regulations*, dated 9-29-06, which outlines the DOE polygraph examination program
DOE Regulation	• Memorandum for the Secretary, SUBJECT: *ACTION: To obtain the Secretary's approval to designate Sigma 20 personnel as subject to mandatory counterintelligence evaluations*, dated 4-11-12 and approved 4-23-12, which forms the basis for current CIEP requirements for personnel authorized access to Sigma 20 NWD • CG-IND-1, *DOE Classification Guide for Improvised Nuclear Devices*, dated October 2006
DOE Orders	• DOE O 457.1, *Nuclear Counterterrorism*, dated 2-7-06, which defines requirements for the protection of sensitive improvised nuclear device information and provides a framework to support DOE activities related to nuclear counterterrorism • DOE M 457.1-1, *Control of Improvised Nuclear Device Information*, dated 8-10-06, which provides requirements and procedures for protecting Sigma 20 information • DOE O 153.1, *Departmental Radiological Emergency Response Assets*, dated 9-20-91, which establishes requirements and responsibilities for the DOE/NNSA national radiological emergency response assets and capabilities and Nuclear Emergency Support Team assets • DOE O 200.1A, *Information Technology Management Program*, dated 12-23-08, and National Archives and Record Administration-approved DOE records schedules, which describe requirements for managing records related to this program • DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, dated 5-14-12, which establishes a general process and provides direction for controlling access to and disseminating Sigmas 14 and 15 NWD at the Department of Energy • DOE O 470.3B, *Graded Security Protection (GSP) Policy* (U), dated 8-12-08 (Secret//RD//NOFORN), 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

	• DOE O 470.4B, *Safeguards and Security Awareness Program*, dated 7-21-11, which establishes the roles and responsibilities for the U.S. Department of Energy Safeguards and Security Program • DOE O 471.6, *Information Security*, dated 6-20-11, 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 • DOE O 472.2, *Personnel Security*, dated 7-27-11, which establishes the overall objectives and requirements for the Department of Energy Personnel Security Program • DOE O 473.3, *Protection Program Operations*, dated 6-29-11, which establishes the requirements for protection of facilities, buildings, and Government property, including classified information, special nuclear materials, and nuclear weapons • 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
Contract Controls	• DOE O 457.1 Contract Requirements Document • DOE M 457.1-1 Contract Requirements Document • Other CRDs associated with directives listed above
External Assessments	• *None*

Risk Mitigation Techniques

[Use the risk mitigation techniques and guidance within the attached reference to fill out the chart below. List all risks that have been identified in the gap analysis. When examining the relative cost-benefit of a proposed control be careful to notice situations where a risk-specific control may also (directly or indirectly) address a separate risk identified in the gap analysis.]

Risk Assessment for [Directive Number, *Directive Title*]					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
1. Risk to personnel from terrorist acts of nuclear sabotage 2. Inability to secure improvised nuclear device and related information 3. Inability to stop terrorist nuclear device from functioning 4. Risk to assets from terrorist acts of nuclear sabotage 5. Cost of decommissioning, decontaminating, or rebuilding facilities, infrastructure, and/or cities following acts of nuclear terrorism 6. Risk to US citizens and USG interests from acts of nuclear terrorism	Significant	(Functioning) Radiation Exposure Device: $1M-100M (Detonated) Radiological Dispersal Device $100M - $10B (Detonated) Improvised Nuclear Device $10B-$10T	Public Law (P.L.) 83-703, the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011) Title XXXII of P.L. 106-65, NN5A Act, as amended National Security Presidential Directive 28, US Nuclear Weapons Command and Control, Safety, and Security (U) 10 CFR 709, *Counterintelligence Evaluation Regulations*	Monitoring, Mitigation, and Avoidance	Maintenance of controls currently in DOE O 457.1, DOE M 457.1-1, CG-IND-1, and other DOE directives Interagency (Work for Others) coordination Counterintelligence Evaluation Program

References

Risk/Opportunity Categories

- People – Risks that affect the individual well being.
- Mission – Risks that impede the ability of the department or offices to accomplish their mission.
- Assets – Risks that impact federal land, buildings, facilities, equipment, etc.
- Financial – Risks that may incur costs or obligations outside of DOE's control.
- Customer and Public Trust – Risks that affect the trust and political environment around DOE.

Probability Ratings

- Rare – even without controls in place, it is nearly certain that event would not occur
- Unlikely – without controls in place, it is unlikely the event would occur
- Possible – without controls in place, there is an even (50/50) probability that the event will occur
- Likely – without controls in place, the event is more likely than not to occur
- Certain – without controls in place, the event will occur

Impact Ratings

Rating	Risk	Opportunity
Negligible	Events of this type have very little short-term or long-term impact and whatever went wrong can be easily and quickly corrected with little effect on people, mission, assets, finances, or stakeholder trust.	A benefit with little no to improvement of operations or utilization of resources.
Low	Events of this type may have a moderate impact in the short term, but can be easily and quickly corrected with no long term consequences.	A benefit with minor improvement of operations or utilization of resources.
Medium	Events of this type have a significant impact in the short term and the actions needed to recover from them may take significant time and resources.	A benefit with somewhat major improvement of operations or utilization of resources.
High	Events of this type are catastrophic and result in long-term impacts that significantly affect the ability of the Department to complete its mission.	A benefit with major improvement of operations or utilization of resources.

Risk Level Ratings

		Impact			
		Negligible	Low	Medium	High
Probability	Certain	Minor	Moderate	Extreme	Extreme
	Likely	Minor	Moderate	Significant	Extreme
	Possible	Minor	Moderate	Significant	Extreme
	Unlikely	Minor	Minor	Moderate	Significant
	Rare	Minor	Minor	Minor	Moderate

Risk Mitigation Options and Guidance

- Acceptance
- Monitoring
- Mitigation
- Avoidance

Unmitigated Risk / Strategy	Extreme	Significant	Moderate	Minor
Acceptance	• Not Appropriate	• Not Appropriate	• Not Appropriate	• Risks can be handled through performance feedback and accountability
Monitoring	• Mandatory Contractor independent assessments • Federal oversight with a mandatory periodicity • Mandatory, periodic reporting	• Mandatory Contractor Self-assessments with a minimum periodicity • Federal oversight with a periodicity that is based on performance • Mandatory, periodic reporting	• Limited Federal oversight based on performance • Mandatory reporting of threshold events	• Federal oversight on a for-cause basis • Standard performance evaluation processes
Mitigation	• Federal approvals of individual transactions • Detailed performance or process requirements • Detailed design requirements	• Federal approvals of systems and programs • Detailed performance or process requirements • Detailed design requirements	• Detailed performance requirements	• General Performance Requirements
Avoidance	• Prohibition of activities or operations	• Prohibition of activities or operations	• Prohibition of activities or operations	• Guidance