

SUPPLEMENTAL DIRECTIVE

NNSA SD 471.6

Approved: 12-09-19
Certification Due: 12-09-22

OPERATIONS SECURITY PROGRAM



NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
<https://directives.nnsa.doe.gov/>

OFFICE OF PRIMARY INTEREST (OPI):
Office of Defense Nuclear Security

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

OPERATIONS SECURITY PROGRAM

1. PURPOSE. This National Nuclear Security Administration (NNSA) Supplemental Directive (SD) defines requirements and responsibilities associated with the implementation of an Operations Security (OPSEC) Program. The objectives are
 - a. to ensure that critical information is protected from inadvertent disclosure.
 - b. to provide management with the information required for sound risk management decisions concerning the protection of sensitive information.
 - c. to ensure that OPSEC techniques and measures are used throughout the nuclear security enterprise.
2. AUTHORITY.
 - a. National Security Decision Directive (NSDD) 298, *National Operations Security Program*, which requires each Executive department and agency assigned or supporting national security missions with classified or sensitive activities to establish a formal OPSEC Program.
 - b. Department of Energy (DOE) Order (O) 471.6 Ch. 2, *Information Security*. No provisions in DOE O 471.6 are contradicted or deleted in this SD.
3. CANCELLATION. None.
4. APPLICABILITY.
 - a. Federal. This SD applies to all federal NNSA elements.
 - b. Contractors. The Contractor Requirements Document (CRD), included as Attachment 1, sets forth requirements of this directive that apply to contractors. The CRD also includes Attachments 2-4 and must be included in Management and Operating contracts and provided to all prime contractors performing work for NNSA, to include publishing information pertaining to mission activities, acquisitions, supply chain, research and design, performance data, and other sensitive activities conducted on behalf of NNSA.
 - c. Equivalencies/Exemptions.
 - (1) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 United States Code sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

- (2) Equivalency and exemption requests are processed through the requirements contained in NNSA Supplemental Directive 470.4-2, *Enterprise Safeguards and Security Planning and Analysis Program*.

5. REQUIREMENTS.

- a. Each site or facility must appoint an OPSEC point of contact (POC) with overall OPSEC responsibilities. OPSEC POC contact information must be provided to the NNSA Office of Defense Nuclear Security (NA-70).
- b. The OPSEC Program must include local site-specific training tailored to the job duties or mission requirements of the site. OPSEC training may be incorporated into existing site training schedules or may be provided separately.
- c. The OPSEC Program must include an annual comprehensive OPSEC-specific briefing. The OPSEC-specific briefing must contain:
 - (1) adversary intent and capability;
 - (2) consequence of loss or compromise;
 - (3) best practices, vulnerabilities, and countermeasures; and
 - (4) critical information.
- d. The OPSEC Program must be reviewed and evaluated for compliance through the established self-assessment process.
- e. Employees with official OPSEC responsibilities must receive formal OPSEC training.
- f. OPSEC plans must be developed and updated or reviewed at least every 12 months.
- g. Critical information must be identified, including operational and programmatic data that would have a negative impact on national security or departmental operations if inadvertent disclosure should occur. The critical information must be:
 - (1) Prioritized according to the level of impact posed by disclosure. The critical information may be supported by a list of OPSEC indicators that, when aggregated and analyzed, inappropriately reveal elements of the critical information.
 - (2) Reviewed on a continuing basis and updated or reviewed at least annually, or as required. The results of the critical information reviews must be documented and maintained in program files.

- h. An OPSEC threat analysis must be documented and include the requirements stated in DOE O 475.1, *Counterintelligence Program*; DOE O 470.3C, *Design Basis Threat*; or any successor documents. The analysis must provide postulated threat information, and serve as the baseline for developing threat analysis. Once developed, the analysis must be reviewed annually and updated as necessary.
- i. An annual schedule of OPSEC assessments must be developed. The priority for conducting OPSEC assessments is based on critical information, threat assessments, risk management principles, and direction from NNSA or contractor line management.
- j. OPSEC assessments must be conducted:
 - (1) At a frequency not to exceed 36 months at facilities having Category I special nuclear material (or credible roll-up of Category II to a Category I quantity), Top Secret, or Special Access Program information within their boundaries.
 - (2) At other facilities involved in creating, handling, storing, processing, transmitting, or destroying critical information as identified in the OPSEC plan.
- k. Either the programmatic or facility approach must be used to conduct OPSEC assessments.
 - (1) If the facility approach is used, all activities at the facility must be included in the assessment.
 - (2) If the programmatic approach is used, all activities within the program must be included in the assessment.
- l. Assessment results and identification of risk must be documented and communicated to the appropriate stakeholders.
- m. OPSEC reviews must be conducted to identify changing priorities in the local OPSEC Program. OPSEC reviews are limited information-gathering activities to provide the data necessary to schedule and implement OPSEC actions. OPSEC reviews will take into consideration many of the same concerns as an OPSEC assessment, but are less intrusive and less detailed. The results of OPSEC reviews must be documented. OPSEC reviews must be conducted when one of the following criteria are met:
 - (1) New construction or major modification is planned for a facility that will process or store classified or sensitive information or matter.
 - (2) New sensitive activities are initiated, or existing programs incur significant changes.

- (3) A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding two years.
- n. Information generated by or for the Federal Government (government information) must not contain critical information when released outside the security boundary. Security boundaries exist in various domains (to include physical and virtual), and vulnerabilities can become apparent as data crosses each boundary. Information and derived products are considered to have passed the security boundary once they are no longer under direct or exclusive control of personnel or infrastructure.
 - (1) Local procedures must be established for conducting information reviews prior to release of information. These procedures must identify specific information and information categories, considered unsuitable for public release.
 - (2) These reviews must be conducted from an OPSEC perspective and are separate from other reviews and determinations, such as classification and *Freedom of Information Act* (FOIA).
 - (3) Due to the diversity of information that must be considered, a robust review and approval process must be conducted using the following evaluation factors to determine suitability for release of information outside of the security boundary. Evaluation factors include:
 - (a) Sensitivity. If the information is released, it must not reveal or identify sensitive or classified information, activities, or programs.
 - (b) Risk. Information that may be used by adversaries to the detriment of employees, the public, the Department, or the Nation must not be approved for release. This determination must be based on sound risk management principles focused on preventing potential adverse consequences in the short and long terms.
- o. OPSEC must be incorporated into the foreign visits and assignment approval process.
- p. OPSEC working group(s) must be established and consist of representatives from various organizational elements.

6. RESPONSIBILITIES.

a. Associate Administrator and Chief, Defense Nuclear Security.

Responsible for the development and implementation of security programs for the Administration, including the protection, control, and accounting of materials, and for the physical security for all facilities of the Administration.

b. Office of Security Operations and Programmatic Planning (NA-71).

- (1) Coordinates with the DOE Office of Counterintelligence for NNSA-wide OPSEC threat purposes.
- (2) Coordinates with internal and external agencies or organizations to represent NNSA interests or concerns.
- (3) Integrates and coordinates information related to the NNSA-wide Critical Information List(s).

c. Office of Resource Management and Mission Support (NA-72).

Establishes and implements an OPSEC Program for NNSA Headquarters elements.

d. NNSA Program and Support Offices.

Assign an OPSEC representative who is responsible for developing, reviewing, and disseminating program-specific critical information associated with their organizational mission, or assist in the development of an NNSA-wide critical information list.

e. Officially Designated Federal Security Authority (ODFSA).

- (1) Implements the OPSEC SD for federal OPSEC programs.
- (2) Approves federal OPSEC plans.
- (3) Monitors implementation of this SD and provides oversight of the contractor OPSEC Program.
- (4) Reviews vulnerabilities resulting from OPSEC reviews or assessments that indicate moderate or high risk.
- (5) Authorizes information generated by or for the Federal Government and being made available to the public that contains Critical Information.

f. Operations Security Point of Contact.

12-09-19

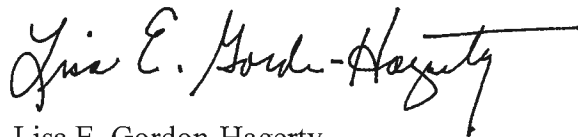
- (1) Implements the requirements and processes associated with the OPSEC Program.
- (2) Establishes working group(s).
- (3) In conjunction with the DOE Office of Intelligence and Counterintelligence, develops threat information to support the OPSEC Program. Other internal and external organizations may also be used to develop site-specific OPSEC threat documents.

g. Contracting Officers.

Incorporate the CRD of this SD into contracts within six months of the effective date of this NNSA directive.

7. DEFINITIONS. See Attachment 2.
8. ACRONYMS/ABBREVIATIONS. See Attachment 3.
9. REFERENCES. See Attachment 4.
10. CONTACT. Questions concerning this SD should be addressed to the Office of Defense Nuclear Security (NA-70) at (202) 586-8900.

BY ORDER OF THE ADMINISTRATOR:



Lisa E. Gordon-Hagerty
Administrator

Attachments:

1. Contractor Requirements Document (CRD)
2. Definitions
3. Acronyms
4. References

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT
NNSA SD 471.6, *OPERATIONS SECURITY PROGRAM*

This Contractor Requirements Document (CRD) establishes enterprise Operations Security (OPSEC) Program requirements for National Nuclear Security Administration (NNSA) contractors performing safeguards and security work for NNSA, to include publishing information pertaining to mission activities, acquisitions, supply chain, research and design, performance data, and other sensitive activities conducted on behalf of NNSA. Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

In addition to the requirements of this CRD, contractors are subject to the information set forth in Attachments 2-4 of SD 471.6.

1. **REQUIREMENTS.**

- a. Each site or facility must appoint an OPSEC point of contact (POC) with overall OPSEC responsibilities. OPSEC POC contact information must be provided to the NNSA Office of Defense Nuclear Security (NA-70).
- b. The OPSEC Program must include local site-specific training tailored to the job duties or mission requirements of the site. OPSEC training may be incorporated into existing site training schedules or may be provided separately.
- c. The OPSEC Program must include an annual comprehensive OPSEC-specific briefing. The OPSEC-specific briefing must contain:
 - (1) adversary intent and capability;
 - (2) consequence of loss or compromise;
 - (3) best practices, vulnerabilities, and countermeasures; and
 - (4) critical information.
- d. The OPSEC Program must be reviewed and evaluated for compliance through the established self-assessment process.
- e. Employees with official OPSEC responsibilities must receive formal OPSEC training.
- f. OPSEC plans must be developed and updated or reviewed at least every 12 months.

- g. Critical information must be identified, including operational and programmatic data that would have a negative impact on national security or departmental operations if inadvertent disclosure should occur. The critical information must be:
 - (1) Prioritized according to the level of impact posed by disclosure. The critical information may be supported by a list of OPSEC indicators that, when aggregated and analyzed, inappropriately reveal elements of the critical information.
 - (2) Reviewed on a continuing basis and updated or reviewed at least annually, or as required. The results of the critical information reviews must be documented and maintained in program files.
- h. An OPSEC threat analysis must be documented and include the requirements stated in DOE O 475.1, *Counterintelligence Program*; DOE O 470.3C, *Design Basis Threat*; or any successor documents. The analysis must provide postulated threat information, and serve as the baseline for developing threat analysis. Once developed, the analysis must be reviewed annually and updated as necessary.
- i. An annual schedule of OPSEC assessments must be developed. The priority for conducting OPSEC assessments is based on critical information, threat assessments, risk management principles, and direction from NNSA or contractor line management.
- j. OPSEC assessments must be conducted:
 - (1) At least once every 36 months at facilities having Category I special nuclear material (or credible roll-up of Category II to a Category I quantity), Top Secret, or Special Access Program information within their boundaries.
 - (2) At other facilities involved in creating, handling, storing, processing, transmitting, or destroying critical information as identified in the OPSEC plan.
- k. Either the programmatic or facility approach must be used to conduct OPSEC assessments.
 - (1) If the facility approach is used, all activities at the facility must be included in the assessment.
 - (2) If the programmatic approach is used, all activities within the program must be included in the assessment.
- l. Assessment results and identification of risk must be documented, and results communicated to the appropriate stakeholders.

- m. OPSEC reviews must be conducted to identify changing priorities in the local OPSEC Program. OPSEC reviews are limited information-gathering activities to provide the data necessary to schedule and implement OPSEC actions. OPSEC reviews take into consideration many of the same concerns as an OPSEC assessment, but are less intrusive and less detailed. The results of OPSEC reviews must be documented. OPSEC reviews must be conducted when one of the following criteria are met:
 - (1) New construction or major modification is planned for a facility that will process or store classified or sensitive information or matter.
 - (2) New sensitive activities are initiated, or existing programs incur significant changes.
 - (3) A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding two years.
- n. Information generated by or for the Federal Government (government information) must not contain critical information when released outside of the security boundary. Security boundaries exist in various domains (to include physical and virtual), and vulnerabilities can become apparent as data crosses each boundary. Information and derived products are considered to have passed the security boundary once they are no longer under direct or exclusive control of personnel or infrastructure.
 - (1) Local procedures must be established for conducting information reviews prior to release of information. These procedures must identify specific information and information categories, considered unsuitable for public release.
 - (2) These reviews must be conducted from an OPSEC perspective and are separate from other reviews and determinations, such as classification and FOIA.
 - (3) Due to the diversity of information that must be considered, a robust review and approval process must be conducted using the following evaluation factors to determine suitability for release of information outside of the security boundary. Evaluation factors include:
 - (a) Sensitivity. If the information is released, it must not reveal or identify sensitive or classified information, activities, or programs.
 - (b) Risk. Information that may be used by adversaries to the detriment of employees, the public, the Department, or the nation must not be approved for release. This determination must be based on sound

risk management principles focused on preventing potential adverse consequences in the short and long terms.

- o. OPSEC must be incorporated into the foreign visits and assignment approval process.
- p. OPSEC working group(s) must be established and consist of representatives from various organizational elements.

2. RESPONSIBILITIES.

- a. Officially Designated Security Authority (ODSA).
 - (1) Implements the OPSEC Supplemental Directive CRD.
 - (2) Approves contractor OPSEC plans.
- b. Operations Security Point of Contact.
 - (1) Implements the requirements and processes associated with the OPSEC Program.
 - (2) Establishes working group(s).
 - (3) In conjunction with the DOE Office of Intelligence and Counterintelligence, develops threat information to support the OPSEC Program. Other internal and external organizations may also be used to develop site-specific OPSEC threat documents.

ATTACHMENT 2: DEFINITIONS

Note: This attachment applies to National Nuclear Security Administration (NNSA) federal and contractor personnel and must be included with the Contractor Requirements Document.

1. Critical Information. Specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives. National Security Decision Directive 298, National Operation Security (OPSEC) Program, OPSEC Glossary of Terms. (DOE O 471.6, *Information Security*).
2. Facility. A facility consists of one or more security interests under a single security management responsibility or authority, and a single facility security officer within a defined boundary that encompasses all the security assets at that location. A facility operates under a security plan that allows security management to maintain daily supervision of its operations, including day-to-day observations of the security program. (DOE O 470.4B, *Safeguards and Security Program*).
3. Inadvertent. An act during which a person carefully follows the prescribed procedures as he or she understands them, but the security interest is mishandled anyway. This type of noncompliance situation arises without any kind of risk/benefit analysis and is generally the result of ignorance of requirements or a systematic or procedural failure (DOE-STD-1210-2012, *Incidents of Security Concern*).
4. Officially Designated Federal Security Authority (ODFSA). Federal employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. Delegation authority for these positions is originated according to direction from the accountable Program Secretarial Officer (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Office), who also provides direction regarding which of the ODFSA positions may be further delegated. Each delegation must be documented in writing. The delegation may be included in other security plans or documentation approved by or according to direction from the accountable principal. Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation (DOE O 470.4B, *Safeguards and Security Program*).
5. Officially Designated Security Authority (ODSA). For purposes of this policy, ODSAs are at the contractor level. This is the level of authority granted to commit security resources, direct the allocation of security personnel, or approve security implementation plans and procedures to accomplish specific work activities.
6. OPSEC Assessment. An assessment conducted to determine whether critical information is vulnerable to exploitation. An OPSEC assessment is a critical analysis of *what we do* and *how we do it* from the perspective of an adversary.
7. OPSEC Indicator. Any detectable activity or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.
8. OPSEC Point of Contact. Individual responsible for the overall day-to-day management and

administration of the local OPSEC Program in compliance with National Security Decision Directive 298, *National Operations Security Program*, DOE O 471.6, *Information Security* and as provided by law or contract. Titles may vary by site.

9. OPSEC Representative. An individual with OPSEC-related responsibilities who contributes to an NNSA-wide critical information list. These individuals are typically designated by Headquarters program offices to represent specific mission areas.
10. OPSEC Review. Broad scope appraisals of a specific facility, program, or activity to determine the level of OPSEC support needed.
11. Publicly Available. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public (DOE Procedures for Intelligence Activities).
12. Public Release. The act of making information available to the general public, usually through an approved process. Public release includes but is not limited to publishing documents on web sites available to the public, information provided to Congress, briefings to audiences that include members of the public, and Freedom of Information Act releases (DOE O 475.2B, *Identifying Classified Information*).

ATTACHMENT 3: ACRONYMS AND ABBREVIATIONS

Note: This attachment applies to NNSA federal and contractor personnel and must be included with the Contractor Requirements Document.

1. CRD Contractor Requirements Document
2. DOE Department of Energy
3. FOIA Freedom of Information Act
4. NNSA National Nuclear Security Administration
5. NSDD National Security Decision Directive
6. O Order
7. ODFSA Officially Designated Federal Security Authority
8. ODSA Officially Designated Security Authority
9. OPSEC Operations Security
10. POC Point of Contact
11. SD Supplemental Directive

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 4: REFERENCES

Note: This attachment applies to National Nuclear Security Administration (NNSA) federal and contractor personnel and must be included with the Contractor Requirements Document.

1. Executive Order 12344, *Naval Nuclear Propulsion Program*, dated 2-1-82
2. National Security Decision Directive 298, *National Operations Security Program*, dated 1-22-88
3. Department of Energy (DOE) Order (O) 142.3A Chg.1, *Unclassified Foreign Visits and Assignments Program*, dated 1-18-17, or successor document
4. DOE O 470.3C, *Design Basis Threat (DBT) Order*, dated 11-23-16, or successor document
5. DOE O 470.4B Chg.2, *Safeguards and Security Program*, dated 1-17-17, or successor document
6. DOE O 471.5, *Special Access Programs*, dated 3-29-11, or successor document
7. DOE O 471.6 Admin Chg 2, *Information Security*, dated 5-15-15, or successor document
8. DOE O 475.1, *Counterintelligence Program*, dated 12-10-04, or successor document
9. DOE O 475.2B, *Identifying Classified Information*, dated 10-02-14, or successor document
10. NNSA Policy 24A, *Weapon Quality Policy*, dated 11-24-15, or successor document
11. NNSA Supplemental Directive 470.4-2, *Enterprise Safeguards and Security Planning and Analysis Program*, dated 6-23-18, or successor document
12. DOE Procedures for Intelligence Activities, dated 1-17-19, or successor document