ORDER

DOE O 471.6

Approved: 6-20-2011

INFORMATION SECURITY

U.S. DEPARTMENT OF ENERGY

Office of Health, Safety and Security

TABLE OF CONTENTS

INFORMATION SECURITY

1. PURPOSE. The protection and control of classified information is critical to our nation's security. This Order establishes requirements and responsibilities for Department of Energy (DOE) Departmental Elements, including the National Nuclear Security Administration (NNSA), to protect and control classified information as required by statutes, regulation, Executive Orders, government-wide policy directives and guidelines, and DOE policy and directives. Such requirements and responsibilities include providing direction to Departmental programs and contractors to ensure that all applicable laws, regulations, policies, directives and other requirements are followed or achieved, and that classified information is properly protected and controlled.

2. CANCELLATION. (DOE M 470.4-4A chg. 1, *Information Security Manual*, dated 10-12-2010, except for Section D – Technical Surveillance Countermeasures, which will be retained in its entirety as the policy referenced in Paragraph 4.g. of this Order.) 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contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.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 Elements.

      (1) Except as otherwise indicated in this section, the requirements in this Order apply to all Departmental Elements that possess, may possess or have authority to possess classified information.

      (2) The Administrator of the NNSA must ensure that NNSA employees comply with their responsibilities under this Directive. Nothing in this Directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of the National Nuclear Security Administration Act ("NNSA Act") (50 U.S.C. § 2402(d)) to establish Administration-specific policies, unless disapproved by the Secretary.

      (3) This Order applies to the Bonneville Power Administration (BPA). The BPA Administrator will assure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA's self financing, procurement and other statutory authorities.

      (4) In accordance with the responsibilities and authorities assigned by the NNSA Act (50 U.S.C. § 2406) and Executive Order 12344 (February 1, 1982), codified 50 U.S.C. § 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.

(5) The requirements in this Order apply to DOE (and DOE contractor) activities and facilities that are subject to licensing and related regulatory authority or certification by the Nuclear Regulatory Commission (NRC). The requirements in this Order should be applied consistent with Executive Order 12829, "Executive National Industrial Security Program" (January 6, 1993), the 1996 "Memorandum of Understanding Between the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission Under the Provisions of the National Industrial Security Program" as may be amended or superseded, and related memoranda of understanding between NRC and DOE concerning classified information, executed in accordance with applicable laws, regulations, policies, directives, and requirements.

(6) Additional direction may apply or take precedence over this Order regarding the possession, handling and control of Sensitive Compartmented Information.

b. DOE Contractors. The CRD, Attachment 1, sets forth requirements that apply to contracts that include the CRD. This CRD, or its requirements, must be included in all contracts that involve classified information and contain DEAR clause 952.204-2, titled Security. A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data (RD) or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

c. Equivalencies/Exemptions for DOE O 471.6. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1C, *Departmental Directive Program*.

When conditions warrant, equivalencies or exemptions from the requirements in this Order, requests must be supported by a vulnerability assessment (VA) when required by the assets being protected, or by sufficient analysis to form the basis for an informed risk management decision, the analysis must identify compensatory measures, if applicable, or alternative controls to be implemented. All approved equivalencies and exemptions under this Order must be entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security plan(s). Approved equivalencies and exemptions become a valid basis for operation when they have been entered in

SSIMS and documented in the appropriate security plan, and they must be incorporated into site procedures at that time.

Many DOE safeguards and security (S&S) Program requirements are found in or based on regulations issued by Federal agencies, and codified in the CFR or other authorities, such as Executive Orders or Presidential Directives. In such cases, the process for deviating from those requirements found in the source document must be applied. If the source document does not include a deviation process, the DOE Office of the General Counsel, or NNSA Office of General Counsel if an NNSA element is involved, must be consulted to determine whether deviation from the source can be legally pursued.

4. REQUIREMENTS.

a. General.

(1) Classified information in all forms must be protected in accordance with all applicable laws, regulations, policies, directives, and other requirements.

(2) NNSA and DOE program offices must provide direction to Federal personnel, contractors, and any other organizational elements to ensure that all DOE and national policies, objectives, and requirements are implemented and achieved. They must also establish or provide direction for establishing each Officially Designated Federal Security Authority (ODFSA) and Officially Designated Security Authority (ODSA) necessary to fulfill their respective roles in accordance with all applicable delegations and authorities.

(3) All procedures utilized to protect classified information must be documented in security plans.

(4) Authorized access to classified information requires appropriate clearance, relevant access approval, and need to know.

(5) All classified information must be protected from unauthorized access.

(6) Methods to deter, detect, respond to, and mitigate unauthorized access to classified information must be implemented.

(7) All classified information, including but not limited to that which is generated, received, transmitted, used, stored, reproduced, or permanently placed (buried according to the requirements of this Order) — until it is destroyed or otherwise no longer classified — must be protected and controlled commensurate with its classification level, category, and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized

access to classified information. (Examples of such attributes include, but are not limited to size, location, and configuration.)

(8) All individuals who are authorized for access to classified information must receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable about their responsibilities and applicable requirements.

b. Handling and Protection. Handling and protection procedures must be established, documented, and adhered to for classified information throughout its lifecycle (which includes origination, classification, marking, accountability, in-use, storage, reproduction, transmission, and destruction).

(1) Origination and Classification.

(a) Prior to classification review, information that may be classified must be protected at the highest potential classification level and category of the information it contains.

(b) The originator must ensure that a derivative or original classifier reviews the information and determines its classification including:

1 When unsure of the classification level or category of a draft or working paper; and

2 For all final products that may contain classified information.

(c) The originator must ensure that all classified matter is appropriately marked according to the classification determination.

(2) Marking.

(a) Marking Standards. Classified matter must include proper and complete classification markings.

1 Classified matter must be reviewed and brought up to current marking standards whenever it is released by the current holder ("current holder" may be an individual, specific office, or ad-hoc working group) or removed from a state of permanent storage and placed into use.

2 When marking the level or category is not practical, written notification of the classification must be furnished to all recipients.

3 Documents that contain Transclassified Foreign Nuclear Information (TFNI) must be marked TFNI following the classification level on the top and bottom of the first page and either on subsequent pages containing TFNI or all pages, unless such documents (or pages) also contain RD or Formerly Restricted Data (FRD). The "Declassify on" line of documents containing TFNI must state "Not Applicable (or N/A) to TFNI." Documents containing TFNI and other NSI, but no RD or FRD must be portion marked. Portions containing TFNI must be marked with the level and with the TFNI identifier (e.g., S/TFNI).

(b) Examples. Marking examples may be found in the CMPC Marking Resource at http://www.hss.energy.gov/secpolicy/DOE_CMPC_Marking_Resource.pdf.

(c) Mixed Levels and Categories. When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. (For example, a document that contains Confidential RD and Secret National Security Information [NSI] would be required to be marked as Secret RD, the highest level and most restrictive category, even though none of the information in the document is Secret RD.)

If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text.

This document contains:

Restricted Data at the *(e.g., Confidential*) level.
Formerly Restricted Data at the (*e.g., Secret*) level.
National Security Information at the (*e.g., Secret*) level.

Classified by: *Name and Title*

(d) Portion Marking. When portion marking is required, classified matter must be marked in a manner that clearly indicates those portions that contain or reveal classified information.

1 NSI documents (including page changes) dated after April 1, 1997, must be portion marked.

2 All NSI documents that are in use (not in approved storage) must be portion marked.

3 Documents containing RD or FRD are not required to be portion marked.

(e) Subjects and Titles. Titles must be marked with the appropriate classification (level; category if RD or FRD; and other applicable caveats) or "U" if unclassified, and the marking must be placed immediately preceding the item.

(f) Transmittal Documents. The first page of a transmittal document must be marked with the highest level; most restrictive category (if RD or FRD); and other applicable caveats of classified information being transmitted and with an appropriate notation to indicate its classification when the enclosures are removed.

(g) Working Papers. In addition to national requirements for working papers, these documents must be marked as "Draft" or "Working Paper" on the front cover until they are marked as final documents. RD and FRD drafts and working papers also must include the same markings as required for NSI drafts and working papers.

Classified documents that are updated on a frequent basis, commonly referred to as "living" documents (e.g., documents that are part of an ongoing experiment or study) may be considered as originating on each date they are changed. Security plans must document specific techniques to demonstrate that working papers and drafts are "living" documents.

(h) Other Government Agencies (OGAs) Not Conforming to DOE Marking Requirements. Documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD) or TFNI identifiers, when applicable.

(i) Foreign Governments Not Conforming to DOE Marking Requirements. Documents received from foreign governments that have not been marked to conform to DOE requirements, do not need to be re marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD) or TFNI identifiers, when applicable.

(j) Cover Sheets. Cover sheets must be applied to all classified documents when they are removed from a secure storage repository (standard form [SF] 703 for Top Secret, SF 704 for Secret, SF 705 for Confidential, and DOE F 470.9 for Confidential

Foreign Government Information–Modified Handling Authorized [C/FGI-MOD]).

(k) Media. When information is prepared on classified information systems, the hard copy output (which includes paper, microfiche, film, and other media) must be correctly marked either according to its classification per review of the output or as a working paper.

(3) Accountability.

(a) The following types of matter are accountable:

1 Top Secret matter;

2 Secret Restricted Data matter stored outside a limited area (LA) or higher; and

3 Any matter designated as accountable by national, international, or programmatic requirements. Examples include, but are not limited to, Sigma 14 and North Atlantic Treaty Organization (NATO) Atomal.

(b) All accountable matter must be managed such that:

1 Chain of custody is established, verified, and documented from origination or receipt to destruction or transfer outside of departmental control;

2 Each accountable item can be located at any given time, whether stored or in use (the location of accountable classified matter in approved permanent burial must be documented, and this matter's unaccessed status must be verifiable); and

3 All discrepancies regarding inventories of accountable matter are detected and reported to the ODFSA.

(4) Classified Information in Use.

(a) When not in approved storage, all classified information must be under the direct control of an individual who meets the requirements for authorized access to the information.

(b) All users of classified information must prevent unauthorized physical, visual, aural, cyber, and other access.

(c) Classified information must only be processed on information systems that have received authority to operate at the appropriate

classification for the information according to DOE Office of the Chief Information Officer directives.

(5) Storage.

(a) Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person.

(b) Requirements for Intrusion Detection Systems (IDS) that are used for supplemental control are established in DOE physical protection directives.

(c) Requirements for vaults and Vault Type Rooms (VTRs) used for open storage of classified matter are established in DOE physical protection directives.

(d) Storage Containers.

1 Storage containers used to store classified matter must not be used to store or contain other items that may be a substantial target for theft.

2 Storage containers used for storing classified matter must conform to U.S. General Services Administration (GSA) standards and specifications.

3 Combinations must be set by an appropriately cleared and authorized individual.

4 Combinations must be changed as soon as practical whenever a current combination may be known by someone who does not possess the requisite access authorization, formal access approvals, and need to know for all of the information stored in the container.

5 A record must be maintained of each individual who has been granted access to any secure storage repository combination.

6 SF 700 Parts 1, 2, and 2A must be completed for each secure storage repository or other location approved for storing classified matter that uses a combination.

a The combination must be available for authorized use.

b The local implementation plan may dictate whether Block 8, Serial Number of Lock, must be left blank.

c SF 700 Part 1 must be affixed to the inside of the door of vaults and VTRs containing the combination lock. For security containers, it must be placed inside the locking drawer.

7 An SF 702 must be used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who has opened, closed, or checked a particular container, room, vault, or VTR holding classified information.

(e) Top Secret matter must be stored in one of the following three ways.

1 In a locked, GSA-approved security container with one of the following supplemental controls:

a Under IDS protection and by protective force (PF) personnel responding within 15 minutes of alarm annunciation; or

b Inspections by PF personnel no less frequently than every 2 hours.

2 In a locked vault or VTR within an LA, exclusion area, protected area (PA), or material access area. The vault or VTR must be equipped with IDS equipment, and PF personnel must respond within 15 minutes of alarm annunciation.

3 In a locked vault or VTR within a property protection area or outside of a security area, and it must be under IDS protection. PF personnel must respond within 5 minutes of alarm annunciation.

(f) Secret matter must be stored:

1 In any manner authorized for Top Secret matter;

2 In a locked vault or in a locked GSA-approved security container within an LA or higher; or

3 In a locked VTR with the following supplemental controls:

a Inspections by PF personnel no less frequently than every 4 hours; or

b For a VTR located within a PA or higher security area, the PF personnel must respond within 30 minutes of the VTR's IDS alarm.

(g) Confidential matter must be stored in the same manner prescribed for Secret or Top Secret matter. However, the supplemental controls are not required.

(h) Nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or VTR located in an LA or higher security area, with:

1 IDS supplemental control; and

2 PF personnel must respond within 15 minutes of the IDS alarm.

(i) PF personnel, private security firms, or local law enforcement agency personnel must respond to IDS alarms as specified and documented in the local security plan.

(j) Nonconforming storage may only be used for classified matter that cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, nonconforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

1 Nonconforming storage must result in protection effectiveness equivalent to that provided to similar levels and categories of classified matter by standard configurations.

2 The methods, protection measures, and procedures must be documented and approved by the ODFSA.

3 Documentation must include the following:

a An explanation as to why exercising this option is necessary;

b A description of the classified matter to be stored; and

c An analysis demonstrating the means by which equivalent security is to be provided.

4 Copies of the documentation must be forwarded to the cognizant Headquarters program office.

(k) Permanent burial is an option that may be approved by the ODFSA for permanent placement of classified matter. Permanent placement is not a form of destruction for classified matter. In addition to meeting the requirements for nonconforming storage of classified matter, permanent burial documentation must also include:

1 For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial;

2 Configuration of classified matter to be buried;

3 Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter; and

4 Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter.

(l) Accountable classified matter is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.

(6) Reproduction. Procedures for the reproduction of classified matter must be established to:

(a) Limit reproduction of classified matter to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations; and

(b) Identify equipment authorized in accordance with local procedures and cyber security policy.

(7) Transmission and Receipt.

(a) Procedures for the transmission and receipt of classified matter must be established to deter, detect, and respond to unauthorized access to the matter. In addition to national requirements, DOE-specific policy includes:

1 Classified mailing addresses must be verified through SSIMS or the listing provided by the Defense Security Service (DSS). If not in either system, a new classified mail channel must be established.

2 Hard copy printouts of SSIMS or DSS classified addresses can only be used to validate approved classified addresses for 30 calendar days from the print date.

3 Receipts must be used to manage and verify timely delivery of matter classified Secret or higher.

4 Classified matter may be transmitted by approved electronic means. When using this method, both the transmitting and receiving systems must be approved for the classification level and category of the information to be transmitted. Facilities also must have an approved security plan and a procedure(s) for transmitting the information by electronic means.

5 First class mail is not authorized for transmission of Top Secret or Secret classified matter. First class mail also may not be used for transmission of Confidential matter to contractor facilities.

6 U.S. Postal Service Express Mail is not authorized for transmission of Top Secret matter, but may be used to transmit Secret or Confidential matter.

7 Unless otherwise noted in this Order, DOE authorizes the use of the current holders of a GSA contract for overnight delivery of information for the Executive Branch as long as all requirements are met.

8 When using commercial express service organizations for transmitting classified matter, the matter must be secured at the receiving location the next calendar day.

a The use of the express service organization must have been approved by the sender's ODFSA.

b An address for receiving deliveries from the express service must have been input into SSIMS for the receiving organization if sending classified information to a DOE cleared site or if sending Restricted Data.

c The delivery address cannot be a post office box and must be a street address.

d The intended recipients must be notified 24 hours in advance (or immediately if transit time is less than 24 hours) of the proposed shipments and arrival dates.

e All packages must be double-wrapped before being inserted into the packaging provided by the commercial express service organization.

f In accordance with packaging requirements, commercial express service packages must not be identified as classified packages.

g The properly wrapped packages must be hand-carried to the express mail dispatch center or picked up from the sender in sufficient time to allow for dispatch on the same day.

h Commercial express carrier drop boxes must not be used for classified packages.

9 Common carriers used to transport classified matter must have an approved facility clearance (FCL) which is also entered into SSIMS.

10 Procedures must be developed describing the process for obtaining approval to hand-carry outside of a site/facility and for providing notification when removing classified matter from the facility. Hand-carry procedures must be approved by the ODSA.

a A record/receipt of the classified matter to be hand-carried must be made before departure.

b The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.

c Contingency plans for delayed arrival must cover alternative protection, storage procedures, and reporting requirements, and they must be approved by the ODSA. Plans must also include disposition/return of the classified matter.

d Requirements for security screening of classified matter at airports are established by the Transportation Security Administration (TSA). Requirements for precluding unauthorized access to classified information apply in addition to those established by TSA.

e To hand-carry classified matter outside the United States, the traveler must obtain written authorization from the cognizant Departmental Element, who must arrange for nonprofessional diplomatic courier status from the U.S. Department of State.

(8) Destruction.

(a) For destruction, classified matter must be destroyed beyond recognition and must not permit subsequent recovery of classified information.

(b) Electronic storage media containing classified information must be destroyed in accordance with DOE cyber security directives.

(c) Destruction of accountable classified matter must be witnessed by an appropriately cleared individual, other than the person destroying the matter, who has an appropriate security clearance for the classification level, category (if RD or FRD), and any applicable caveats of the matter to be destroyed.

c. Foreign Government Information.

(1) Foreign Government Information (FGI) must be safeguarded to provide a degree of protection at least equivalent to that required by the government, international organization of governments, or any element thereof that furnished the information.

(2) FGI to which U.S. information has been added must be reviewed for classification by a derivative classifier or classification officer, marked, and protected accordingly.

(3) Confidential Foreign Government Information–Modified Handling Authorized (C/FGI-MOD). The Information Security Oversight Office provides requirements that must be met when the foreign protection requirements are lower than the protection required for U.S. Confidential information.

(4) NATO information must be safeguarded in compliance with the U.S. Security Authority for NATO Affairs instructions.

(5) Modifications to these requirements regarding FGI may be permitted by treaties, agreements, or other obligations with the prior written consent of the originating government.

(6) Release or Disclosure of FGI.

(a) The release or disclosure of any FGI must have the prior consent of the originating government, must be coordinated through the cognizant DOE Program Office and Office of Health, Safety and Security, and must comply with all applicable treaties, agreements, or other obligations.

(b) Any individual receiving FGI must possess an appropriate security clearance and meet need-to-know requirements.

(c) If the release or disclosure involves FGI produced by or received from an OGA, approval must be obtained from that OGA before release or disclosure.

d. Release or Disclosure of U.S. Classified Information to Foreign Governments.

(1) The multiagency National Disclosure Policy Committee (NDPC), of which DOE is a Special Member, governs the export of classified U.S. military information and material to foreign governments as provided for in international agreements. The NDPC must be informed of international agreements involving the sharing of all classified information with foreign governments, including those international agreements made under the auspices of the Atomic Energy Act of 1954, as amended. This notification must include the provisions of security agreements that apply to the shared information. Disclosure of atomic information (which includes RD and FRD) must be coordinated with the Joint Atomic Information Exchange Group before disclosure.

(2) Before releasing classified information to any foreign government, DOE must determine that furnishing the classified information will result in a net advantage to the national security of the United States and comply with all applicable treaties, agreements and other obligations. These determinations must be made in coordination with the appropriate DOE Program Office.

(3) Before releasing classified information to any foreign government, the receiving government must have agreed, in writing, to the following stipulations:

(a) The receiving foreign government must not release the information to a third party without the written approval of the releasing party;

(b) The receiving foreign government will protect the information to the same degree of protection as that provided by the releasing party.

(c) The receiving foreign government will use the information only for the purpose for which it was given.

(d) If the releasing party indicates any private rights (such as patents, copyrights, or trade secrets) are involved in the information, the receiving foreign government will acknowledge such rights.

(4) In some instances, new documents may be created that contain both U.S. classified information and FGI. In this case, unless there is a current agreement for cooperation (for RD or FRD) or an appropriate international agreement (for NSI) allowing sharing of the specific categories and levels of U.S. classified information, the enhanced FGI cannot be returned to the originating government or international organization of governments.

(5) All transmittals to a foreign government that involve classified information must be made by DOE unless a DOE contractor has prior written authorization.

(6) The method of transmission of classified mail to any foreign government must be approved by the Office of Health, Safety and Security.

(7) Copies of receipts for physical transfer of classified information to foreign entities must be contained in memoranda prepared by the Cognizant Departmental Element and maintained by the cognizant program office.

(8) Records of made and/or contemplated oral disclosures must be contained in memoranda prepared by the Cognizant Departmental Element and maintained by the cognizant program office.

e. Disclosure and Release in Emergency Situations. In the event that an emergency situation necessitates the disclosure of classified information to individuals who are not otherwise eligible for access, the following requirements apply. If any of these requirements are not met, the DOE or NNSA Office of the General Counsel, as appropriate, must be consulted as soon as possible.

(1) Protection.

(a) The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum necessary.

(b) If classified information must be transmitted, it must be transmitted via approved channels if possible or through the most secure and expeditious method if approved channels are not an option.

(c) A written description detailing what information is classified and the protection requirements for that information must be provided to the recipient.

(d) A briefing must be provided to the recipient(s) covering requirements for not disclosing the information.

(e) A nondisclosure agreement signed by the recipient(s) must be obtained.

(2) Notification and Reporting. The following individuals must be notified as soon as possible of any emergency release of classified information to an individual or individuals who are otherwise not eligible for such access:

(a) For RD or FRD: the Chief Health, Safety and Security Officer; the head of the Departmental Element; and the Associate Administrator for Defense Nuclear Security; or

(b) For NSI: the appropriate DOE line management or ODFSA.

f. Operations Security (OPSEC).

(1) An OPSEC program(s) must be implemented covering each site and facility to ensure the protection of Critical Information (CI) and to enhance mission effectiveness and protection of operations and activities.

(2) Each OPSEC program must:

(a) Identify and document its CI;

(b) Review and update its CI documentation as necessary to reflect current assets, threats, operations and other relevant factors;

(c) Ensure that its CI is protected from inadvertent and unauthorized disclosure, commensurate with all pertinent factors;

(d) Provide the information required for sound risk-management decisions concerning the protection of sensitive information to the decision makers who are responsible for mission accomplishment; and

(e) Assign and document approved responsibilities for OPSEC direction, management, and implementation.

(3) OPSEC assessments must be conducted at a frequency not to exceed 36 months at facilities that possess Category I special nuclear material (or credible roll up to a Category I quantity), Top Secret, or Special Access Program information within their boundaries.

(4) Information generated by or for the Federal Government and being placed on any website or otherwise being made available to the public must not contain CI unless authorized by the ODFSA.

g. Technical Surveillance Countermeasures. Copies of the DOE Technical Surveillance Countermeasures policy are controlled and may be requested from the DOE Office of Health, Safety and Security at (301) 903-9992.

5. RESPONSIBILITIES.

a. Office of Health, Safety and Security.

(1) Develops, coordinates, and interprets the Department's information security policy consistent with strategies and policies governing the protection of national security and other critical assets entrusted to the Department.

(2) Designates the senior agency official responsible for directing and administering the DOE information security program, pursuant to Executive Order 13526, section 5.4(d).

(3) Approves the methods of transmission of classified mail to foreign governments.

(4) Coordinates with program offices regarding the release or disclosure of FGI.

(5) Coordinates with program offices regarding the release or disclosure of classified information to foreign government(s).

(6) Maintains documentation for emergency disclosures involving RD or FRD.

(7) Fulfills program office responsibilities for security at DOE Headquarters.

b. Office of the Chief Information Officer.

(1) Provides DOE directives for protection and handling of cyber forms of classified information.

(2) Provides DOE directives for the security of the information systems that store classified information.

(3) Provides DOE directives to ensure that classified information is only processed on information systems that achieve the appropriate requirements for national security systems.

c. Program Secretarial Offices. Establish implementing direction to their Program Offices to ensure that all applicable laws, regulations, policies, directives and other requirements are followed or achieved, and that classified information is properly protected and controlled.

d. DOE Program Offices.

(1) Implement the senior agency official's policies for directing and administering the DOE information security program (Executive Order 13526, section 5.4(d)).

(2) Provide implementing direction to their organizations and contractors to ensure that all applicable laws, regulations, policies, directives and other requirements are followed or achieved.

(3) Approve release or disclosure of FGI.

(4) Manage and approve the release and disclosure of U.S. classified information to foreign governments.

(5) Maintain documentation for emergency disclosures involving NSI, RD, and FRD.

(6) Designate information security authorities and define their roles and responsibilities for their programs, sites, facilities, and operations.

(7) Ensure that contracting officers incorporate the CRD and all program-specific implementing instructions, into those contracts that involve classified information, classified matter or nuclear materials and contain DEAR clause 952.204 2, Security Requirements.

(8) Ensures that approved documentation for their programs, sites, facilities, and operations is developed and maintained, including, but not limited to the following:

(a) Security plans;

(b) Nonconforming storage;

(c) Release and disclosure of FGI;

(d) Transport of classified information by a specific individual(s) outside the United States; and

(e) Copies of receipts for physical transfer of classified information to foreign governments.

e. NNSA.

(1) Provides decisions, direction and guidance regarding the senior agency (DOE) official's policies for directing and administering the DOE information security program for NNSA offices and programs (Executive Order 13526, section 5.4(d)).

(2) Provides implementing direction to NNSA organizations and contractors to ensure that all applicable laws, regulations, policies, directives, and other requirements are followed or achieved.

(3) Manages and approves the release and disclosure of NNSA classified information to foreign country governments.

(4) Maintains documentation for emergency disclosures involving NSI, RD, and FRD.

(5) Designates information security authorities and defines their roles and responsibilities, within NNSA.

(6) Ensures that contracting officers incorporate the CRD and all program-specific implementing instructions, into those contracts that involve classified information, classified matter or nuclear materials and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled Security Requirements.

(7) Ensures that approved documentation for their programs, sites, facilities and operations is developed and maintained, including, but not limited to the following:

(a) Security plans;

(b) Nonconforming storage;

(c) NNSA release and disclosure of FGI;

(d) Transport of classified information by a specific individual(s) outside the United States; and

(e) Copies of receipts for physical transfer of classified information to foreign governments.

f. ODFSAs and ODSAs. Fulfill requirements and responsibilities that are delegated to them.

g. Contracting Officers. Upon notification, modify contracts to incorporate program-specific implementing instructions from NNSA and DOE program offices into those contracts that involve classified information, classified matter or nuclear materials and contain DEAR clause 952.204-2, titled Security Requirements.

6. REFERENCES. The following tools may assist in locating DOE and national directives that have requirements that apply to the information security topical area. The documents provided within each tool may not be the official versions of the associated laws, policy and requirements documents, and directives. The current official version of any requirements directives must be used when developing policy or procedures. Links or references to the official documents or their websites are provided when available.

a. The Policy Information Resource provides a keyword search to retrieve a list of documents containing the keyword(s) entered. The Policy Information Resource also supports browsing directives or collections of driver documents. It also contains a glossary and acronym collection. The resource may be accessed at: http://pir.pnl.gov.

b. The DOE CMPC Marking Resource is an Office of Health, Safety and Security resource and provides examples for marking classified documents. The *CMPC Marking Resource* can be accessed at: http://www.hss.doe.gov/SecPolicy/DOE_CMPC_Marking_Resource.pdf.

7. DEFINITIONS. For purpose of this order, the following definitions apply.

a. Access. The ability or opportunity to gain knowledge of classified information.

b. Classified Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that has been determined pursuant to executive order, regulation or statute to meet classification requirements.

c. Classified Matter. Anything in physical form that contains or reveals classified information.

d. 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.

e. Foreign Government Information. Foreign Government Information as defined in Section 6.1(s) of Executive Order 13526.

f. Officially Designated Federal Security Authority (ODFSA). ODFSAs are 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 for which of the ODFSA positions may be further delegated. Each delegation must be documented in written form. It 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 delegatee's acts or omissions in carrying out the purpose of the delegation.

g. Officially Designated Security Authority (ODSA). ODSAs are Federal or contractor employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation.

Delegation of 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 for which of the ODFSA positions may be further delegated. Each delegation must be documented in written form. It 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 delegatee's acts or omissions in carrying out the purpose of the delegation.

h. Transclassified Foreign Nuclear Information. Information concerning the atomic energy programs of other nations that has been removed from the Restricted Data category for use by the intelligence community and is safeguarded as NSI under E.O. 13526. Documents marked as containing TFNI are excluded from the automatic declassification provisions of the Order until the TFNI designation is properly removed by the Department of Energy.

8. CONTACT. For information about this Order, contact the Office of Health, Safety and Security at: (301) 903-0292.

BY ORDER OF THE SECRETARY OF ENERGY:

DANIEL B. PONEMAN
Deputy Secretary

ATTACHMENT 1. CONTRACTOR REQUIREMENTS DOCUMENT

Regardless of the performer of the work, the contractors must comply with the requirements of this contractor requirements document and with National Nuclear Security Administration (NNSA) and other Department of Energy (DOE) program office direction provided through contract. Each contractor is responsible for disseminating the requirements and NNSA or other DOE program office direction to subcontractors at any tier to the extent necessary to ensure the contractor's and subcontractor's compliance with the requirements.

Contractors must protect and handle classified information and critical information in accordance with applicable laws, regulations, policies, directives and other requirements as directed through contract by the NNSA or other DOE program office(s).

A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, Procedural Rules of the Assessment of Civil Penalties for Classified Information Security Violations.