DOE M 470.4-7

Approved: 08-26-05

SAFEGUARDS AND SECURITY PROGRAM REFERENCES

DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

SECTION B – SAFEGUARDS AND SECURITY REFERENCES

This Section contains S&S references arranged as general references and by topical S&S programmatic areas. These references are currently used in S&S directives. As with the *Glossary*, revisions to this Section are encouraged and should be submitted to the Office of Security.

Safeguards and Security General References

1. United States Code (U.S.C.).

   a. 5 U.S.C. 552, *The Freedom of Information Act*, as amended, which requires Federal agencies to make information available upon request by anyone, subject to certain exemptions and exceptions.

   b. 5 U.S.C. 552a, *The Privacy Act of 1974*, as amended, which limits Federal agencies on establishing and releasing records on individuals and granting access to such records, and establishes certain rights concerning one's records.

   c. 42 U.S.C. 2011 to 2296, which is the codification of the *Atomic Energy Act of 1954 (AEA)*, and which establishes several programs related to atomic energy, including a program for Federal control of the possession, use, and production of nuclear energy and special nuclear material (SNM), whether owned by the Government or others.

      (1) 42 U.S.C. 2161 to 2166 (Sections 141 to 146, as amended, *AEA*), which sets requirements for Restricted Data.

      (2) 42 U.S.C. 2201 (Section 161, as amended, *AEA*), which sets out the general duties of DOE, including the issuance of regulations and directives to protect the common defense and security.

      (3) 42 U.S.C. 2271 to 2181 (Sections 221 to 233, as amended, *AEA*), which gives the FBI the authority to investigate alleged or suspected criminal violations of the Act, makes violations of the Act criminal, and provides for injunction and contempt proceedings.

      (4) 42 U.S.C. 2282b (Section 234B, as amended, *AEA*), which establishes civil penalties for violations of directives regarding protection of classified information by contractors or their employees.

   d. 42 U.S.C. 7101 to 7386k, which is the principal codification of the *Department of Energy Organization Act*, and which establishes DOE and its basic authorities and responsibilities, including the responsibility of the Secretary for developing and promulgating DOE security policies (42 U.S.C. 7144a).

e. 50 U.S.C. 2401 to 2484, and 42 U.S.C. 7132, 7133, 7144, and 7158, all of which codify the *National Nuclear Security Administration Act*, and which establish the National Nuclear Security Administration within DOE and its authorities and responsibilities.

2. Executive Orders (E.O.), Office of the President.

a. E.O. 12829, *National Industrial Security Program*, 1-6-93, as amended by E.O. 12885, 12-14-93, which establishes the National Industrial Security Program (NISP) to protect classified information released by Federal agencies to their contractors, directs the Secretary of Defense to issue the NISP Operating Manual, and makes the Director of the Information Security Oversight Office (ISOO) responsible for implementing and monitoring the NISP Government-wide; however, DOE and NRC retain authority over access to information classified under the Atomic Energy Act of 1954.

b. E.O. 12958, *Classified National Security Information*, as amended (see E.O. 13292, 3-25-03), which prescribes a uniform system for classifying, protecting, and declassifying National Security Information.

c. E.O.12968, *Access to Classified Information*, 8-2-95, which establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

3. Title 10, Code of Federal Regulations (CFR), *Energy*.

a. 10 CFR Part 710, Subpart A, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*, which establishes criteria and procedures for resolving questions concerning eligibility for a DOE access authorization.

b. 10 CFR Part 712, *Human Reliability Program*, which establishes a safety and security program by requiring those in positions with access to certain materials, devices, facilities, and programs to meet reliability, physical, and mental suitability standards, and by evaluating them to identify those whose judgment or reliability may pose a safety or security concern.

c. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, which establishes rules to assess a penalty for violation of a directive relating to the protection of classified information pursuant to 42 U.S.C. 2282b [Section 234B, as amended, of the *Atomic Energy Act of 1954*] or for violation of a compliance order that directs corrective action for the protection of classified information.

4. 32 CFR Chapter XX, *Information Security Oversight Office, National Archives and Records Administration.*

a. 32 CFR Part 2001, *Classified National Security Information* (which is the Information Security Oversight Office's (ISOO) *Classified National Security Information Directive Number 1*, 9-22-03), which addresses protection of National Security Information.

b. 32 CFR Part 2003, *National Security Information – Standard Forms*, which prescribes standard forms for use in the protection of National Security Information.

5. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation* (DEAR), which supplements 48 CFR Chapter 1, *Federal Acquisition Regulation*, and includes the security clauses to be used in DOE solicitations and contracts or agreements involving access to classified information and/or a significant quantity of SNM.

a. 48 CFR 904.404, *Solicitation Provision and Contract Clause*, which lists the solicitation provision that should be used when contract performance will involve access authorizations, the contract clauses that must be inserted when performance will involve classified information, and the contract clauses that either should or must be inserted when classified information will not be involved, but certain unclassified controlled information may be. These provisions are described below.

(1) 48 CFR 952.204-2, *Security Requirements*, which contains a contract clause that must be used when performance involves classified information. The clause's provisions require compliance with security requirements, the return of classified information and special nuclear material at contract termination, and compliance with foreign ownership, control, or influence requirements.

(2) 48 CFR 952.204–70, *Classification/Declassification*, which contains a contract clause that must be used when performance involves classified information. The clause's provisions require submission of material to derivative classifier for review, review of classified holdings for declassification purposes, and insertion of the clause in subcontracts that involve classified information.

(3) 48 CFR 952.204–71, *Sensitive Foreign Nation Controls*, which is a clause that is required in unclassified research contracts which may involve making unclassified information about nuclear technology available to certain sensitive foreign nations.

(4) 48 CFR 952.204-72, *Disclosure of Information*, which is a clause used in contracts with educational institutions that are not likely to produce classified information, but establishes what must be done if classified information becomes involved in the contract.

(5) 48 CFR 952.204-73, *Facility Clearance*, which is a clause which must be used in solicitations expected to result in contracts that require employees to possess access authorizations.

(6) 48 CFR 952.204-76, *Conditional Payment of Fee or Profit – Safeguarding Restricted Data or Other Classified Information*, which is a clause used in certain contacts that involve classified information, but do not contain a nuclear hazards indemnity clause.

b. 48 CFR Subpart 904.70, *Facility Clearances*, which sets forth requirements and procedures regarding facility clearances for contractors and subcontractors that require access to classified information or special nuclear material.

c. 48 CFR Part 970, *DOE Management and Operating Contracts,* which are special DEAR provisions applicable to management and operating contracts.

(1) 48 CFR 970.0404-4, *Solicitation Provision and Contract Clauses,* which requires use of the solicitation provision and contract clauses in 48 CFR 904.404.

(2) 48 CFR 970.0470-2, *Contract Clause,* which requires use of the contract clause in 48 CFR 970.5204-2.

(3) 48 CFR 970.5204-2, *Laws, Regulations and DOE Directives,* which is a contract clause that requires compliance with laws, regulations, and if a list is appended to the contract, specified DOE directives; prescribes the process for changing the list, and requires the contractor to flow down these requirements to subcontractors.

6. National Industrial Security Program, Department of Defense (DoD).

a. DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995, which implements E.O. 12958 by prescribing requirements to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by Federal agencies to their contractors.

b. DoD 5220.22-M-Sup 1, *National Industrial Security Program Operating Manual Operating Manual Supplement,* February 1995, as amended, which establishes enhanced security requirements for special access programs and sensitive compartmented information.

7. DOE O 142.3, *Unclassified Foreign Visits and Assignments,* 6-18-04, which establishes authorities, responsibilities, and policy, and prescribes administrative procedures for visits and assignments by foreign nationals to DOE facilities.

8. DOE O 200.1, *Information Management Program,* 9-30-96, which establishes responsibilities for information management and provides a framework for managing information and information resources.

9. DOE M 200.1-1, *Telecommunications Security Manual,* 3-1-97, which provides for the Communications Security program, including protection of crypto facilities.

10. DOE O 231.1A, *Environment, Safety, and Health Reporting,* 6-3-04, which implements statutory and regulatory reporting requirements, and requirements to keep management informed on a timely basis of adverse or potentially adverse events affecting the environment, safety, or health.

11. DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information,* 8-19-03, which establishes a system for reporting occurrences related to DOE-owned or operated facilities and processing that information to provide for appropriate corrective action.

12. DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy,* 5-8-01, which establishes a formal ISSM framework for use in systematically integrating S&S into management and work practices at all levels so that missions are accomplished securely.

13. DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, 10-31-02, which establishes responsibilities and requirements for independent evaluation of the adequacy of policy and the effectiveness of line management performance in S&S.

14. DOE O 470.3, *Design Basis Threat Policy* (U), 10-1-04, which identifies and characterizes the potential generic adversary threats to the DOE programs and facilities which could adversely impact national security, the health and safety of employees, the public, or the environment. The directive is available from the Office of Security to cleared personnel with a need-to-know.

15. DOE O 470.4, *Safeguards and Security Program*, which establishes the roles and responsibilities for S&S programs.

16. DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, which establishes general requirements for S&S planning and for the following programs: Foreign Ownership, Control, or Influence; S&S Training; S&S Awareness; Control of Classified Visits; Deviations; and Incidents of Security Concern.

17. DOE M 470.4-2, *Physical Protection*, which prescribes the requirements and detailed procedures for the Physical Protection Program.

18. DOE M 470.4-3, *Protective Force*, which prescribes requirements and detailed procedures for the Protective Force Program.

19. DOE M 470.4-4, *Information Security*, which prescribes requirements for the Information Security Program.

20. DOE M 470.4-5, *Personnel Security*, which prescribes the requirements for implementing the Personnel Security Program.

21. DOE M 470.4-6, *Nuclear Material Control and Accountability*, which prescribes requirements and procedures for the Nuclear Material Control and Accountability Program.

22. DOE M 470.4-7, *Safeguards and Security Program References*, which provides a Glossary for S&S Program terms and their definitions, and provides references, acronyms, and abbreviations applicable to the S&S directives.

23. DOE O 475.1, *Counterintelligence Program*, 12-10-04, which establishes responsibilities, requirements, and definitions for the Counterintelligence Program.

24. DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01, which provides requirements for managing the DOE classification and declassification program, including details for classifying and declassifying information, documents, and material.

25. DOE 3750.1, *Work Force Discipline*, 3-23-83, which establishes penalties for employees who violate laws or regulations.

26. Records Schedules.

a. General Records Schedule 18, *Security and Protective Services Records,* National Archives and Records Administration Transmittal No. 8, December 1998, which provides disposition authorization for Federal records related to security and protective services.

b. DOE Administrative Records Schedule 18, *Security, Emergency Planning, and Safety Records,* 1-23-04, Office of the Chief Information Officer, which supplements General Records Schedule 18.

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*

Section A – Safeguards and Security Program Planning

1. DOE O 470.3, *Design Basis Threat Policy* (U), 10-1-04, which identifies and characterizes the potential generic adversary threats to the DOE programs and facilities which could adversely impact national security, the health and safety of employees, the public, or the environment. The directive is available from the Office of Security to cleared personnel with a need-to-know.

Section B – Security Conditions

1. Presidential Directives, Office of the President

   a. Homeland Security Presidential Directive-3 (HSPD-3), *Threat Conditions and Associated Protective Measures,* 3-11-02.

   b. Presidential Decision Directive 39 (PDD-39), *U.S. Policy on Counterterrorism* (U), 6-21-95, which sets policy to deter and respond to terrorist attacks on U.S. territory and against U.S. citizens and facilities worldwide.

Section C – Site Safeguards and Security Plans

1. Technology Transfer Manuals, Sandia National Laboratories.

   a. SAND 2001-2168, *Access Delay,* Volume I, August 2001, which defines the role of barriers in a physical protection program, provides penetration times for barriers, and defines methods for upgrading existing barriers.

   b. SAND99-2390/UC-515, *Alarm Communication and Display,* September 1999, which describes the hardware and implementation techniques for an alarm communication and display system.

   c. SAND 2000-2142, *Entry Control Systems,* 9-30-00, which compiles information regarding entry control systems and their application to physical protection programs.

   d. SAND99-2486, *Explosive Protection,* 8-30-99, which defines explosions and the types of explosives, and the DOE strategy for detection and prevention of the introduction of explosives.

e. SAND99-2391, *Exterior Intrusion Detection*, 8-30-99, which discusses classes of detection systems, how to select the proper sensors, and how to combine them into an effective perimeter subsystem.

f. SAND99-2388, *Interior Intrusion Detection*, 8-30-99, which discusses the broad spectrum of sensors available, the physical principles by which each sensor operates, how the sensors interact with an intruder and the environment, and how the sensors interconnected with the system are monitored and assessed.

g. SAND99-2392, *Protecting Security Communications*, 8-30-99, which discusses the functions of a security communications network, its susceptibility to disruption, and the means by which security radio communications may be protected.

h. SAND99-2389, *Video Assessment*, 8-30-99, which discusses the design and uses of video alarm assessment systems, layouts, location of video system controls, and common construction and installation requirements and techniques.

Section D – Site Safeguards and Security Plan/Resource Plan

None.

Section E – Vulnerability Assessment Program

1. DOE O 470.3, Design Basis Threat Policy (U), 10-01-04, which identifies and characterizes the potential generic adversary threats to the DOE programs and facilities which could adversely impact national security, the health and safety of employees, the public, or the environment. The directive is available to cleared personnel with a need-to-know from the Office of Security.

2. Adversary Capabilities List (U), February 2004, Office of Security and Safety Performance Assurance.

3. Vulnerability Assessment Guide, 9-30-04, Office of Security and Safety Performance Assurance.

Section F – Performance Assurance Program

None

Section G – Survey, Review, and Self-Assessment Program

1. Executive Order 12958, *Classified National Security Information,* as amended (see E.O. 13292, 3-25-03), which requires self-inspections.

   a. Section 5.1(a)(3), which requires the Information Security Oversight Office to develop standards for self-inspection of classified information programs.

   b. Section 5.4(d)(4), which requires agencies to establish and maintain on-going self-inspection programs which include a periodic review and assessment of the agency's classified product.

2. 32 CFR Part 2001, Subpart E, *Self-Inspections* [part of *Classified National Security Information Directive Number 1*, Information Security Oversight Office (ISOO)], which sets standards for establishing and maintaining an internal review and evaluation of the implementation of the classified information program.

3. DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995, Section 1-207.b., *Contractor Reviews,* which requires formal self-inspections.

Section H – Foreign Ownership, Control, or Influence Program

1. 10 U.S.C. 2536(a), which prohibits, unless a waiver is granted by the Secretary, the award of DOE contracts to an entity controlled by a foreign government if it is necessary for that entity to be given access to proscribed information.

2. 50 U.S.C. App. 2170, which prohibits entities controlled by a foreign government from merging with, acquiring, or taking over a U.S. company that either is performing a DOE or DoD contract under a national security program that cannot be performed unless that entity is given access to proscribed information or has DoD or DOE prime contracts totaling more than a half billion dollars.

3. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation* (DEAR), which sets forth the security clauses to be used in DOE solicitations and contracts or agreements involving access to classified information and/or a significant quantity of SNM. Those pertinent to FOCI are:

   a. 48 CFR 904.7002, *Definitions,* which defines "foreign interest" and "Foreign Ownership, Control, or Influence."

   b. 48 CFR 904.7003, *Disclosure of Foreign Ownership, Control, or Influence,* which requires every contractor required to have a facility clearance to provide information relating to foreign ownership, control, or influence (FOCI) at the outset or during the contract performance, and for DOE to make a determination and take action if FOCI exists.

   c. 48 CFR 904.7004, *Findings, Determinations, and Contract Award or Termination,* which establishes DOE procedures for handling FOCI disclosures

   d. 48 CFR Subpart 904.71, *Prohibition on Contracting (National Security Program Contract)*, which implements the prohibition in Section 836 of the 1993 Defense Authorization Act [10 U.S.C. 2536(a)] against the award of a DOE national security contract that results in disclosure of proscribed information to an entity controlled by a foreign government, unless the Secretary waives the prohibition.

   e. 48 CFR 952.204-2, *Security Requirements,* which contains a contract clause that must be used when performance involves classified information. The clause's provision (j), *Foreign Ownership, Control, or Influence,* details a contractor's FOCI requirements

4. DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995.

   a. Section 2-102.d., *Eligibility Requirements (for a Facility Security Clearance)*, which prohibits processing a contractor for a facility security clearance if granting such a

clearance would be inconsistent with the national interest because of the degree to which the contractor is under foreign ownership, control, or influence.

b. Chapter 2, *Facility Clearances, Section 3, Foreign Ownership, Control, or Influence*, which establishes detailed requirements concerning the initial and continuing eligibility of U.S. companies with foreign involvement; the criteria for determining whether U.S. companies are under foreign ownership, control, or influence (FOCI); responsibilities for FOCI matters; and security measures that may negate or reduce FOCI security risks to an acceptable level.

5. DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, 1-24-05, which establishes responsibilities and requirements for the performance of work for non-DOE entities by DOE/NNSA and/or their contractors or the use of DOE/NNSA facilities that is not directly funded by DOE appropriations.

Section I – Facility Clearances and Registration of Safeguards and Security Activities

1. 10 CFR Chapter X, *Department of Energy (General Provisions).*

a. 10 CFR Part 1016, *Safeguarding of Restricted Data*, which establishes requirements for granting security facility approval to an access permittee.

b. 10 CFR Part 1045, *Nuclear Classification and Declassification*, which establishes a program for the managing, identifying, generating, reviewing, and declassifying Restricted Data and Formerly Restricted Data, and the sanctions for violations of the procedures.

2. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation* (DEAR).

a. 48 CFR Subpart 904.70, *Facility Clearances*, which sets forth DOE requirements and procedures regarding facility clearances for contractors and subcontractors that require access to classified information or special nuclear material.

b. 48 CFR 952.204-2(a), *Security Requirements*, which requires contract provisions when performance involves, or is likely to involve, classified information that require compliance with security requirements and the return of classified information at contract termination unless specifically authorized otherwise.

c. 48 CFR 952.204–73, *Facility Clearance*, which is a provision used in solicitations expected to result in contracts and subcontracts that require employees to possess access authorizations.

3. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995.

a. Section 1-302.h., *Changed Conditions Affecting the Facility Security Clearance*, which establishes requirements for reporting significant events affecting the facility contractor.

b. Chapter 2, *Facility Clearances*, which establishes detailed requirements for granting and administering facility clearances.

4. DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work*), 1-24-05, which establishes responsibilities and requirements for the performance of work for non-DOE entities by DOE/NNSA and/or their contractors or the use of DOE/NNSA facilities that is not directly funded by DOE appropriations.

5. DOE O 483.1, *DOE Cooperative Research and Development Agreements*, 1-12-01, which establishes responsibilities and requirements for the oversight, management, and administration of CRADA activities at DOE facilities.

Section J – Safeguards and Security Training Program

1. 5 U.S.C. 4103, *Establishment of Training Programs*, which provides authority for agencies to establish training plans and to establish, operate, maintain, and evaluate training programs for employees in and under the agency.

2. DOE O 360.1B, *Federal Employee Training*, 10-11-01, which establishes requirements and assigns responsibilities for DOE Federal employee training, education, and development under the Government Employees Training Act of 1958.

3. DOE M 360.1-1B, *Federal Employee Training Manual*, 10-11-01, which provides detailed requirements to supplement DOE O 360.1B.

4. DOE 5480.20A, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities*, 7-12-01, which establishes selection, qualification, and training requirements for management and operating contractor personnel involved in the operation, maintenance, and technical support of Category A and B reactors and non-reactor nuclear facilities.

Section K – Safeguards and Security Awareness Program

1. Executive Orders (E.O.) and Presidential Directives, Office of the President.

   a. National Security Decision Directive 84, *Safeguarding National Security Information*, 3-11-83, which requires an individual to sign a nondisclosure agreement and to be apprised of requirements governing contacts with the media before being granted access to classified information.

   b. Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*, 8-5-93, which establishes the responsibility for maintaining a formalized security and/or counterintelligence awareness program directed at foreign and inadvertent disclosure threats, foreign travel briefings on the threat posed by foreign intelligence services, and a means for employees to report hostile contacts.

   c. E.O. 12958, *Classified National Security Information*, as amended (see E.O. 13292, 3-25-03).

      (1) Section 4.1(b), which requires briefings of cleared personnel.

      (2) Section 5.1(a)(3), which establishes the Information Security Oversight Office (ISOO) with authority to issue binding directives on other agencies and standards for briefings.

(3) Section 5.2(b), which authorizes ISOO to oversee agencies' actions.

(4) Section 5.4(d), which requires agencies to designate a senior official with responsibility for establishing and maintaining briefing programs.

d. E.O.12968, *Access to Classified Information*, 8-2-95.

(1) Section 1.5, *Employee Education and Assistance*, which requires a briefing of cleared personnel.

(2) Section 6.1, *Agency Implementing Responsibilities*, which requires continuing security awareness programs.

2. 32 CFR Chapter XX, *Information Security Oversight Office, National Archives and Records Administration.*

a. 32 CFR Part 2001, Subpart F, *Security Education and Training*, which sets the standards for cleared Federal employees, requires maintenance of program records, and requires initial, annual refresher, and termination briefings for cleared employees.

b. 32 CFR 2003.20, *Classified Information Nondisclosure Agreement*, which requires cleared personnel to sign the agreement and makes use of the "debriefing" portion of the agreement optional.

3. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, as amended.

a. Section 1-206, *Security Training and Briefings*, which establishes responsibility for contractors, licensees, or permit holders to provide all cleared employees comprehensive, refresher, and termination briefings.

b. Chapter 3, *Security Training and Briefings*, which establishes requirements for nondisclosure agreements and comprehensive, refresher, and termination briefings for cleared contractor employees

4. DOE O 475.1, *Counterintelligence Program*, 12-10-04, which establishes responsibilities and requirements for the Counterintelligence Program, including counterintelligence briefings and foreign travel briefings/debriefings.

5. *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet*, Information Security Oversight Office, January 2001, which provides information for briefing or giving to personnel who are asked to sign the nondisclosure agreement.

Section L – Control of Classified Visits Program

1. 42 U.S.C. 2163 (Section 143, as amended, of the *Atomic Energy Act of 1954*), which establishes the authority for DOE to permit Department of Defense employees, contractor employees, and Armed Forces members to have access to Restricted Data.

2. 42 U.S.C. 2455(b) (Section 304(b) of the *National Aeronautics and Space Act of 1958*) which controls DOE policy on permitting NASA employees and contractors to have access to Restricted Data.

3. E.O. 12958, *Classified National Security Information*, as amended (see E.O. 13292, 3-25-03), which establishes general restrictions on access to classified information (Section 4.1).

4. DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995, as amended, Section 6-101, *Notification and Approval of Classified Visits*, which details for contractors, licensees, or permit holders the determinations that must be made and requirements that must be met before a classified visit takes place.

5. DOE O 142.1, *Classified Visits Involving Foreign Nationals*, 1-13-04, which establishes responsibilities and requirements for classified visits by foreign nationals.

6. DOE 5610.2, *Control of Weapon Data*, 8-1-80, which establishes responsibilities and requirements for classified visits involving Weapon Data.

Section M – Deviations

None.

Section N – Incidents of Security Concern

1. Title 18 U.S.C., *Crimes and Criminal Procedure,* relating to the following specific crimes:

   a. Espionage (sections 792 to 798).

   b. Treason and subversive activity (sections 2381 to 2385).

   c. Sabotage (sections 2151 and 2153 to 2156).

   d. Theft or destruction of Government property (sections 33, 81, 641, 659, 831, 844, 1361 to 1363, 1366, 2071, 2112, and 2114).

   e. Extortion and threats (sections 876 to 878).

   f. Riots (section 2101).

   g. Crime against a person (sections 111, 113, 114, 351, 1111, 1112, 1114, and 2111.).

   h. Conspiracy (section 371).

   i. Counterfeit badge/identification (sections 499, 701, 911, and 912).

2. 42 U.S.C. 2011 *et seq*. [*Atomic Energy Act of 1954 (AEA),* as amended].

   a. 42 U.S.C. 2271b (Section 221b, as amended, *AEA*), which requires the Federal Bureau of Investigation to investigate all alleged or suspected criminal violations of the *AEA*.

b. 42 U.S.C. 2271c (Section 221c, as amended, *AEA*), which allows administrative action by DOE for violations, but requires the Attorney General to commence any legal action.

3. 50 U.S.C. 47a concerning illegal introduction, manufacture, acquisition, or export of special nuclear materials or atomic weapons, or conspiracies relating thereto.

4. Executive Orders (E.O.) and Presidential Directives, Office of the President.

a. E.O. 12958, *Classified National Security Information*, as amended (see E.O. 13292, 3-25-03), which requires action for violation or infraction of its requirements.

(1) Section 5.5(e)(1), which requires appropriate and prompt action when a violation or infraction occurs.

(2) Section 5.5(e)(2), which requires agencies to notify the Director of the Information Security Oversight Office when certain violations occur.

b. National Security Decision Directive (NSDD) 84, *Safeguarding National Security Information*, 3-11-83, which sets requirements for procedures governing reporting and responding to unauthorized disclosures and authorizes agencies to adopt policies that require employees to submit to polygraphs in the course of unauthorized disclosure investigations.

5. 32 CFR 2001.47, *Loss, Possible Compromise or Unauthorized Disclosure* [part of *Classified National Security Information Directive Number 1*, Information Security Oversight Office (ISOO)], which requires DOE to conduct an inquiry into a loss, possible compromise, or unauthorized disclosure of National Security Information and conduct an assessment of the damage to national security.

6. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, Chapter 1, Section 3, *Reporting Requirements.*

a. Section 1-300, *General*, which establishes responsibility for contractors to report events that affect their facility clearance, the access authorizations of their employees, the protection of classified information in their possession, and indications of loss or compromise of classified information.

b. Section 1-301, *Reports to be Submitted to the FBI*, which requires contractors to report actual or suspected espionage, sabotage, or subversive activities to the FBI with a copy to DOE.

c. Section 1-302, *Reports to be Submitted to the CSA* (Cognizant Security Agency), which requires contractors to report certain information concerning cleared employees or the facility clearance to DOE.

d. Section 1-303, *Reports of Loss, Compromise, or Suspected Compromise*, which requires contractors to conduct preliminary inquiries and issues reports concerning the loss or compromise of classified matter.

7. DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, 3-22-01, which establishes requirements and procedures for reporting fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement to the Office of Inspector General.

8. DOE O 221.3, *Cooperation with the Office of Inspector General*, 3-22-01, which establishes policy for cooperation with the Office of the Inspector General.

9. DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, 8-19-03, which provides detailed information for reporting occurrences and managing associated activities at DOE/NNSA facilities.

10. DOE O 442.1A, *Department of Energy Employee Concerns Program*, 6-6-01, which establishes responsibilities and requirements for ensuring that employees have free and open expression of their concerns related to such issues as the environment, safety, health, and management of DOE/NNSA programs and facilities and that the concerns are addressed through prompt identification, reporting, and resolution that results in an independent, objective evaluation.

11. DOE G 442.1-1, *Department of Energy Employee Concerns Program Guide*, 2-01-99, which provides guidance for implementing DOE O 442.1A.

12. DOE 3750.1, *Work Force Discipline*, 3-23-83, which establishes responsibilities and requirements for disciplining certain employees for the purposes of correcting: unacceptable conduct, behavior on the job, or situations that adversely affect job performance; and violations of laws or regulations.

13. DOE 3771.1, *Grievance Policy and Procedures*, 7-2-81, which establishes responsibilities and requirements for an administrative grievance system available to most employees for a concern or dissatisfaction relating to employment, including matters which the employee alleges have resulted in coercion, reprisal, or retaliation, and for which there is no other established procedure for appeal or complaint.

Section O – Restrictions on the Transfer of Security-Funded Technologies Outside the Department and Its Operational Facilities

None.

DOE M 470.4-2, *Physical Protection*

1. 42 U.S.C. 2278a, *Trespass upon Installations*, which establishes the authority to issue regulations relating to dangerous weapons, explosives, or other dangerous instruments or material likely to produce substantial injury or damage to persons or property at DOE facilities, the penalties for violating these regulations, and the requirement to post the regulations.

2. 42 U.S.C. 7270b, *Trespass on Strategic Petroleum Reserve Facilities*, which authorizes issuance of regulations concerning control of the Strategic Petroleum Reserve.

3. Title 10, Code of Federal Regulations, *Energy*.

   a. 10 CFR Part 712, *Human Reliability Program*, which establishes a safety and security

program by requiring those in positions with access to certain materials, devices, facilities, and programs to meet reliability, physical, and mental suitability standards, and by evaluating them to identify those whose judgment or reliability may pose a safety or security concern.

b. 10 CFR Part 860, *Trespassing on Department of Energy Property*, which prohibits unauthorized entry and unauthorized weapons or dangerous material at DOE facilities.

c. 10 CFR Part 862, *Restrictions on Aircraft Landing and Air Delivery at DOE Nuclear Sites*, which sets security policy regarding aircraft at nuclear sites.

d. 10 CFR Part 1048, *Trespassing on Strategic Petroleum Reserve Facilities and Other Property*, which prohibits unauthorized entry and unauthorized weapons or dangerous material at the Strategic Petroleum Reserve facilities.

4. 41 CFR 102.74, *Facility Management*, which establishes requirements for managing Federal buildings and grounds.

5. DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 11-18-02, provides the construction requirements for the protection of classified information requiring extraordinary security protection.

6. DOE O 151.1B, *Comprehensive Emergency Management System*, 10-29-03, which establishes roles, responsibilities, and requirements for the system.

7. DOE M 200.1-1, *Telecommunications Security Manual*, 3-1-97, which establishes requirements for protection of classified and other sensitive information disclosed in telecommunications.

8. DOE M 411.1-1C, *Safety Management Functions, Responsibilities, and Authorities Manual*, 12-31-03, which sets safety requirements for DOE senior management who have line, support, oversight, and enforcement responsibilities.

9. DOE O 420.1A, *Facility Safety*, 5-20-02, which establishes facility safety requirements.

10. DOE O 420.2B, *Safety of Accelerator Facilities*, 7-23-04, which establishes accelerator-specific safety requirements which, when supplemented by other applicable safety and health requirements, will serve to prevent injuries and illnesses associated with accelerator operations.

11. DOE P 441.1, *DOE Radiological Health and Safety Policy*, 4-26-96, which establishes the basis for DOE's Radiological Control Programs.

12. DOE P 450.2A, *Identifying, Implementing and Complying with Environment, Safety and Health Requirements*, 5-15-96, which sets forth the framework for identifying, implementing and complying with environment, safety and health requirements so that work is performed in the DOE complex in a manner that ensures adequate protection of workers, the public and the environment.

13. DOE P 450.4, *Safety Management System Policy,* 10-15-96, which provides a formal, organized process whereby people plan, perform, assess, and improve the safe conduct of work.

14. DOE O 460.2A, *Departmental Materials Transportation and Packaging Management*, 12-22-04, which sets responsibilities and requirements for nuclear materials transportation on-site.

15. DOE G 460.2-1, *Implementation Guide for Use with DOE O 460.2, Departmental Materials Transportation and Packaging Management*, 11-15-96, which provides guidance for nuclear materials transportation on-site.

16. DOE M 471.2-3A, *Special Access Program Policies, Responsibilities, and Procedures,* 7-11-02, which is an Official Use Only document available from the Office of Security.

17. DOE 1450.4, *Consensual Listening-in to or Recording Telephone/Radio Conversations*, 11-12-92, which specifies when and how a Federal radio or telephone system may be monitored or recorded.

18. *DOE Sensitive Compartmented Information Facility Procedural Guide*, Office of Intelligence, 2-2-00, which implements the appropriate portions of DCIDs.

19. Technology Transfer Manuals, Sandia National Laboratories.

    a. SAND 2001-2168, *Access Delay*, Volume I, August 2001, which defines the role of barriers in a physical protection program, provides penetration times for barriers, and defines methods for upgrading existing barriers.

    b. SAND99-2390/UC-515, *Alarm Communication and Display,* September 1999, which describes the hardware and implementation techniques for an alarm communication and display system.

    c. SAND 2000-2142, *Entry Control Systems*, 9-30-00, which discusses entry control systems and their application to physical protection programs.

    d. SAND99-2486, *Explosive Protection*, 8-30-99, which defines the types of explosives, and the DOE strategy for detection and prevention of the introduction of explosives.

    e. SAND99-2391, *Exterior Intrusion Detection*, 8-30-99, which discusses classes of detection systems, how to select the proper sensors, and how to combine them into an effective perimeter subsystem.

    f. SAND99-2388, *Interior Intrusion Detection*, 8-30-99, which discusses the broad spectrum of sensors available, the physical principles by which each sensor operates, how the sensors interact with an intruder and the environment, and how sensors interconnected with the system are monitored and assessed.

    g. SAND99-2392, *Protecting Security Communications*, 8-30-99, which discusses the functions of a security communications network, its susceptibility to disruption, and the means by which security radio communications may be protected.

h. SAND99-2389, *Video Assessment*, 8-30-99, which discusses the design and uses of video alarm assessment systems, layouts, location of video system controls, and common construction and installation requirements and techniques.

20. General Services Administration, which sets Federal standards and specifications for use by all agencies

a. Federal Standard 809, *Neutralization and Repair of GSA Approved Containers*, 4-1-98.

b. Federal Specification FF-L-2740A, *Locks, Combination*, 1-12-97.

c. Federal Specification FF-P-110J(1), *Padlock, Changeable Combination (Resistant to Opening by Man)*, 1-20-04.

21. Naval Construction Battalion Center, 1000 23rd Avenue, Port Hueneme, CA 93403-4301.

a. MIL-DTL-29181, *Hasp, High Security, Shrouded, for High and Medium Security Padlocks*, 3-10-98.

b. MIL-DTL-43607H, *Padlock, Key Operated, High Security, Shrouded Shackle*, 3-10-98.

22. Special Publication 960-5, *Rockwell Hardness Measurement of Metallic Materials*, January 2001, National Institute of Standards and Technology, Superintendent of Documents, U.S. Government Printing Office, Mail Stop: SSOP, Washington, D.C. 20402-0001.

23. Underwriters Laboratories Inc. (UL), 333 Pfingsten Road, Northbrook, IL 60062.

a. UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*, 2-26-99.

b. UL 752, *Standard for Safety for Bullet-Resisting Equipment*, 3-10-00.

c. UL 827, *Standard for Safety for Central-Station Alarm Services*, 10-1-96.

24. ASTM International, 100 Barr Harbor Drive, P.O. Box C700, Conshohocken, PA 19428-2959.

a. ASTM E413-04, *Classification for Rating Sound Insulation*, 2005, which provides methods of calculating single-number acoustical ratings for laboratory and field measurements of sound attenuation obtained in one-third octave bands.

b. ASTM F792-01e2, *Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*, 2005, which establishes methods for evaluating the systems to determine their applicable performance levels.

25. NFPA-101, *Life Safety Code*, 2003, National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169.

26. American National Standards Institute, Inc., 25 West 43rd Street, 4th Floor, New York, NY 10036.

a. ANSI 156.2-1996, *Grade 1, Bored and Preassembled Locks and Latches,* 1996.

b. ANSI 156.13-1996, *Grade 1, Mortise Locksets.*

27. International Organization for Standardization, 1 Rue de Varembe, Geneva 20, Switzerland.

a. ISO/IEC 7811-6, *Identification Cards – Recording Technique – Part 6: Magnetic Stripe – High Coercivity,* 2001.

b. ISO/IEC 7816-2, *Identification Cards – Integrated Circuit Cards, Part 2: Cards with Contacts – Dimensions and Location of the Contacts,* 1999, with Amendment 1, 2004.

DOE M 470.4-3, *Protective Force*

1. Title 18 U.S.C., *Crimes and Criminal Procedure,* relating to the following specific crimes:

a. Espionage (sections 792 to 798).

b. Treason and subversive activity (sections 2381 to 2385).

c. Sabotage (sections 2151 and 2153 to 2156).

d. Theft or destruction of Government property (sections 33, 81, 641, 659, 831, 844, 1361 to 1363, 1366, 2071, 2112, and 2114).

e. Extortion and threat (sections 876 to 878).

f. Civil disorder and riot (sections 231 and 2101).

g. Crime against a person (sections 111, 113, 114, 351, 1111, 1112, 1114, and 2111).

h. Conspiracy (section 371).

i. Counterfeit badge/identification (sections 499, 701, 911, and 912).

j. False statement (section 1001).

2. 18 U.S.C. 3053, which authorizes U.S. marshals and their deputies to carry firearms and make arrests without warrants for any Federal offense committed in their presence, or for any felony cognizable under Federal laws if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony.

3. 31 U.S.C. 1535 (*Economy Act),* which allows orders to be placed within an agency or with another agency for goods or services when in the best interest of the Government.

4. 42 U.S.C. 2011 *et seq*. [*Atomic Energy Act of 1954 (AEA*), as amended].

a. 42 U.S.C. 2161 to 2166 (Sections 141-146, as amended, *AEA*), which sets forth the principles for the control of Restricted Data.

b. 42 U.S.C. 2201k (Section 161k, as amended, *AEA*), which provides authority for DOE and contractor personnel to carry firearms and to make arrests without warrant.

c. 42 U.S.C. 2271 to 2281 (Sections 221 to 233, *AEA*), which provides authority to investigate and prosecute violations of the Act and to protect Restricted Data and property, and establishes criminal penalties for violations of the Act.

(1) 42 U.S.C. 2271 (Section 221, as amended, *AEA*), which provides the President authority to utilize any agency to protect Restricted Data and DOE property, and requires the FBI to investigate alleged or suspected criminal violations of the Act.

(2) 42 U.S.C. 2272 (Section 222, as amended, *AEA*), which provides penalties for violations of specific sections of the Act concerning unauthorized dealings in SNM, atomic weapons, and utilization or production facilities [42 U.S.C. 2077, 2122, and 2131, respectively (Sections 57, 92, and 101, as amended, *AEA*)], or conspiracy during war or national emergency to interfere with certain DOE actions [42 U.S.C. 2138 (Section 108, as amended, *AEA*)].

(3) 42 U.S.C. 2273 (Section 223, as amended, *AEA*), which provides penalties for violations of any Act provision for which there is no specific penalty; for any violations that occur in connection with construction of or supply of components to a utilization facility, and for violations by individuals indemnified under an agreement of indemnification.

(4) 42 U.S.C. 2274 to 2277 (Sections 224 to 227, as amended, *AEA*), which provides penalties for unauthorized communication, receipt, or disclosure of, or tampering with, Restricted Data.

(5) 42 U.S.C. 2278 (Sections 228 to 230, *AEA*), which provides authority to issue regulations relating to the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any DOE property. It also establishes penalties for violating such regulations and for photographing or making any graphical representation of any installation or equipment designated by the President as protected.

(6) 42 U.S.C. 2279 (Sections 231, as amended, *AEA*), which provides that the Act's provisions do not exclude other applicable laws.

(7) 42 U.S.C. 2280 to 2281 (Sections 232 to 233, *AEA*), which provides for injunction and contempt proceedings related to violations of the Act.

(8) 42 U.S.C. 2282 (Section 234, *AEA*), which provides civil penalties for violations of licensing requirements, safety regulations, and security regulations related to classified and unclassified controlled information.

(9) 42 U.S.C. 2283 (Section 235, *AEA*), which provides criminal penalties for acts against a nuclear inspector.

(10) 42 U.S.C. 2284 (Section 236, as amended, *AEA*), which establishes criminal penalties for destroying or damaging DOE nuclear facilities or fuel, using or tampering with machinery to cause an unauthorized interruption of normal operations of such facilities, or attempting to commit any of these acts.

5. 42 U.S.C. 7270a, which provides authority for DOE and contractor employees at the Strategic Petroleum Reserve to carry firearms and to make arrests without warrant.

6. 50 U.S.C. 797, which provides penalties for violations of DoD security regulations.

7. Presidential Directives, Office of the President.

a. National Security Decision Directive-281, (classified title), 8-27-87, which codifies policies for national nuclear command and control operations.

b. Presidential Decision Directive-39, *U.S. Counterterrorism Policy*, 6-21-95, which establishes policy, requirements, and responsibilities to deter, defeat, and respond to terrorist attacks on U.S. territory and provides resources.

8. Title 10, Code of Federal Regulations (CFR), *Energy*.

a. 10 CFR Part 860, *Trespassing on Department of Energy Property*, which makes trespassing on posted DOE property criminal.

b. 10 CFR Part 1046, *Physical Protection of Security Interests*, which sets policies and procedures applicable to DOE contractor protective force personnel and establishes requirements for their medical and physical fitness qualification, physical fitness training, medical examination and certification, access authorization, and security training, qualifications, and certification.

c. 10 CFR Part 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*, which establishes policy concerning arrests and associated use of force by DOE and contractor protective force personnel assigned to protect nuclear weapons, special nuclear material, classified matter, nuclear facilities, and related property.

d. 10 CFR Part 1049, *Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve*, which establishes policy concerning arrests and associated use of force by Strategic Petroleum Reserve protective force officers and requirements for their training and qualification to carry firearms.

9. Title 14, Code of Federal Regulations (CFR), *Aeronautics and Space*.

a. 14 CFR Part 61, *Certification: Pilots, Flight Instructors, and Ground Instructors*, which prescribes the requirements for issuing pilot and flight instructor certificates and ratings, the conditions under which those certificates and ratings are necessary, and the privileges and limitations of those certificates and ratings.

b. 14 CFR Part 135, *Operating Requirements: Commuter and On-Demand Operations and Rules Governing Persons on Board Such Aircraft*, which governs helicopter operations.

10. Title 29, Code of Federal Regulations (CFR), *Labor*.

a. 29 CFR 1910.95, *Occupational Noise Exposure*, which prescribes when protection against noise exposure must be provided, engineering measures that must be taken when certain sound levels are exceeded, and when hearing conservation programs must be implemented.

b. 29 CFR 1910.1025, *Lead*, which regulates occupational exposure to lead.

11. Title 48, Code of Federal Regulations (CFR), *Federal Acquisition Regulations System.*

a. Subpart 6.3, *Other than Full and Open Competition*, which establishes the circumstances when acquisitions other than through full and open competition may be justified.

b. Subpart 17.5, *Interagency Acquisitions under the Economy Act*, which implements the Economy Act.

12. 49 CFR Part 173, *Shippers – General Requirements for Shipment and Packaging*, which is called the Hazardous Materials Regulations and sets the requirements for preparing hazardous materials for shipment and for the shipping containers.

13. DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, 8-19-03, which establishes a system for reporting occurrences related to DOE facilities and processing that information to provide for appropriate corrective action.

14. DOE O 360.1B, *Federal Employee Training*, 10-11-01, which establishes requirements and assigns responsibilities for DOE Federal employee training, education, and development under the Government Employees Training Act of 1958.

15. DOE O 440.1A, *Worker Protection Management for DOE Federal and Contractor Employees*, 3-27-98, which establishes in Attachment 1, paragraph 3, protective force firearms program safety requirements and responsibilities.

16. DOE M 440.1-1, *DOE Explosives Safety Manual*, 9-30-95, which provides requirements for the safe use and storage of explosives.

17. DOE O 440.2B, *Aviation Management and Safety*, 11-27-02, which provides aviation responsibilities and requirements.

18. DOE O 460.2A, *Departmental Materials Transportation and Packaging Management*, 12-22-04, which establishes policy for and implementation of the management and operation of the Transportation Safeguards System program.

19. DOE G 473.2-1, *Guide for the Establishment of a Contingency Protective Force*, 3-27-03, which provides guidance on establishing and deploying a contingency protective force during an emergency and sustaining operations.

20. DOE-STD-1091-96, *Firearms Safety*, February 1996, which provides principles and practices for protective force firearms safety programs.

21. DoD 6055.9-STD, *DoD Ammunition and Explosives Safety Standards*, 10-4-04, which establishes uniform safety standards for ammunition and explosives.

22. NIJ Standard–0101.04, Revision A, *Ballistics Resistance of Personal Body Armor*, June 2001, Office of Law Enforcement Standards, 100 Bureau Dr., M/S 8102, Gaithersburg, MD 20899-8102.

23. ANSI Z87.1, *Occupational and Educational Personal Eye and Face Protection Devices*, 2003, American National Standards Institute, Inc., 25 West 43rd Street, 4th Floor, New York, NY 10036.

24. UL 752, *Standard for Bullet-Resisting Equipment*, 3-10-00, Underwriters Laboratories Inc. (UL), 333 Pfingsten Road, Northbrook, IL 60062.

25. NFPA-101, *Life Safety Code*, 2003, National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169.

DOE M 470.4-4, *Information Security*

General

1. Executive Order 12829, National Industrial Security Program, 1-6-93, as amended by E.O. 12885, 12-14-93, which establishes a program to protect classified information that is released to Federal contractors, licensees, and grantees and is implemented by the National Industrial Security Program Operating Manual.

2. DOE O 200.1, Information Management Program, 9-30-96, which establishes responsibilities for information management topics and provides a framework for managing information, information resources, and information technology investment.

3. DOE M 200.1, Telecommunications Security Manual, 3-1-97, which establishes requirements for protection of classified and other sensitive information disclosed in telecommunications.

Section A – Classified Matter Protection and Control

1. 18 U.S.C. 798, *Disclosure of Classified Information*, which provides for enforcement and penalties for crimes relating to the disclosure of classified information.

2. 42 U.S.C. 2011 *et seq*. [*Atomic Energy Act of 1954(AEA)*, as amended].

   a. 42 U.S.C. 2161 (Section 141, *AEA*), *Policy*, which prohibits the exchange of Restricted Data with other nations, except as authorized by 42 U.S.C. 2164.

b. 42 U.S.C. 2163 (Section 143, as amended, *AEA*), *Access to Restricted Data,* which provides for the authorization of personnel and contractors to release Restricted Data to DoD personnel, contractors, and military members.

c. 42 U.S.C. 2164 (Section 144, as amended, *AEA*), *International Cooperation,* which allows the President to authorize DOE and other agencies to release certain Restricted Data to foreign countries.

d. 42 U.S.C. 2165 (Section 145, as amended, *AEA*), *Security Restrictions,* which requires contractors and prospective contractors to agree in writing that Restricted Data will not be disseminated to uncleared personnel, and authorizes DOE to release Restricted Data during war or national disasters to persons awaiting access authorizations.

e. 42 U.S.C. 2274 (Section 224, as amended, *AEA*), *Communication of Restricted Data,* which establishes criminal penalties for disclosing Restricted Data with intent to injure the U.S. or aid a foreign country (up to life imprisonment) or with reason to believe it will be used to injure the United States or aid a foreign country (up to 10 years imprisonment and $100,000 fine).

f. 42 U.S.C. 2277 (Section 227, as amended, *AEA*), *Disclosure of Restricted Data,* which establishes criminal penalties of up to a $12,500 fine for disclosing Restricted Data by a Federal or contractor employee to any person who he/she knows or has reason to believe is not authorized to receive it.

g. 42 U.S.C. 2282b (Section 234B, *AEA*), *Civil Monetary Penalties for Violations of DOE Regulations Regarding Security of Classified or Sensitive Information or Data,* which makes any contractor or subcontractor liable to a civil penalty up to $100,000 when they or their employees violate any applicable regulation or directive relating to the protection of classified or sensitive information.

3. Executive Orders (E.O.) and Presidential Directives, Office of the President.

a. E.O. Order 12958, *Classified National Security Information,* as amended (see E.O. 13292, 3-25-03), which requires protection of National Security Information (NSI).

(1) Section 4.1, *General Restrictions on Access,* which establishes who may have access to NSI, standards for access, control of NSI within an agency, protection of foreign government information, and restrictions on dissemination of classified information.

(2) Section 4.2, *Distribution Controls,* which limits distribution to those with access and need-to-know, except during an emergency, when need-to-know may be enough.

(3) Section 5.1, *Program Direction,* which requires the Information Security Oversight Office to publish implementing directives for the protection of classified information that include handling, storage, distribution, transmittal, destruction, and accounting procedures.

(4) Section 5.4, *General Responsibilities,* which requires heads of agencies with classified information to commit management and resources to ensure implementation.

(5) Section 5.5, *Sanctions,* which requires actions against those who knowingly or negligently contravene the Order or implementing directives.

b. National Security Decision Directive (NSDD 84*), Safeguarding National Security Information,* 3-11-83, which sets the requirements for protecting NSI against unlawful disclosures.

4. Title 10, Code of Federal Regulations (CFR), *Energy*.

a. 10 CFR Part 725, *Permits for Access to Restricted Data,* which establishes procedures and standards for the issuance of access permits to persons who require access to Restricted Data that is applicable to the civil uses of atomic energy.

b. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations,* which establishes procedures pursuant to 10 U.S.C. 2282b for assessing civil penalties against a contractor when it or its employees violate DOE directives relating to the protection of Restricted Data or other classified information and for issuing compliance orders by the Secretary for corrective action if an act or omission has created a risk of unauthorized disclosure even if there is no violation of a regulation.

c. 10 CFR, Part 1016, *Safeguarding of Restricted Data,* which establishes requirements for the protection of Restricted Data in connection with an access permit.

d. 10 CFR, Part 1044, *Security Requirements for Protected Disclosures under Section 3164 of the National Defense Authorization Act for Fiscal Year 2000,* which sets requirements for the protected disclosure of classified information under the whistleblower protection granted by Section 3164.

e. 10 CFR, Part 1045, *Nuclear Classification and Declassification,* which establishes the process and rules for the classification and declassification of Restricted Data and Formerly Restricted Data, and penalties for violations.

5. 32 CFR Chapter XX, *Information Security Oversight Office, National Archives and Records Administration.*

a. 32 CFR Part 2001, *Classified National Security Information* (which is the

Information Security Oversight Office's (ISOO) *Classified National Security Information Directive Number 1*, 9-22-03), which addresses protection of National Security Information.

(1) 32 CFR 2001.40, *General*, which provides requirements for using alternative measures for protecting classified information.

(2) 32 CFR 2001.43(b), *Requirements for Physical Protection*, which establishes the requirements to protect each classification level.

(3) 32 CFR 2001.43(c), *Combinations*, and (d), *Key Operated Locks*, which establishes rules on locks.

(4) 32 CFR 2001.44(a), *General*, which requires technical, physical, and personnel control measures for classified information to limit access to authorized personnel, or administrative control measures if the other measures are insufficient to deter unauthorized access.

(5) 32 CFR 2001.44(b), *Reproduction*, which establishes rules on reproduction of classified material.

(6) 32 CFR 2001.45, *Transmission*, which establishes detailed rules depending on transmitting method and destination of classified material.

(7) 32 CFR 2001.46, *Destruction*, which establishes rules for the destruction of classified material.

(8) 32 CFR 2001.47, *Loss, Possible Compromise or Unauthorized Disclosure*, which requires reporting, inquiry or investigation of classified information loss, possible compromise, or unauthorized disclosure, and, when a criminal violation is suspected, coordination with the Department of Justice and DOE legal counsel.

(9) 32 CFR 2001.51, *Emergency Authority*, which addresses release of classified information during an emergency.

(10) 32 CFR 2001.53, *Foreign Government Information*, which sets protection standards for foreign government information.

b. 32 CFR Part 2003, *National Security Information – Standard Forms (SF)*, which prescribes standard forms for use in the protection of National Security Information.

(1) 32 CFR 2003.3, *Waivers*, which provides for waivers from use of the forms.

(2) 32 CFR 2003.21, *Security Container Information: SF 700*, which establishes the requirements to provide contacts for when a security container is found open.

(3) 32 CFR 2003.22, *Activity Security Checklist: SF 701*, which establishes rules for use when conducting daily security checks on areas.

(4) 32 CFR 2003.23, *Security Container Check Sheet: SF 702*, which requires use of a form when accessing, securing, and checking security containers.

(5) 32 CFR 2003.24, *TOP SECRET Cover Sheet: SF 703;* 32 CFR 2003.25, *SECRET Cover Sheet: SF 704;* and 32 CFR 2003.26, *CONFIDENTIAL Cover Sheet: SF 705*, which require use of the appropriate form on classified documents until they are destroyed.

(6) 32 CFR 2003.27, *TOP SECRET Label: SF 706;* 32 CFR 2003.28, *SECRET Label: SF 707;* and 32 CFR 2003.29, *CONFIDENTIAL Label: SF 708*, which require the use of the appropriate label on classified media until it is destroyed.

(7) 32 CFR 2003.30, *CLASSIFIED Label: SF 709*, which requires use of the label on classified media pending a classifier's determination of the classification level.

(8) 32 CFR 2003.31, *UNCLASSIFIED Label: SF 710*, which requires use of the label on unclassified media that is processed or stored in the same environment as classified media.

6. 48 CFR 952.204 (DEAR 952.204), *Clauses Related to Administrative Matters*, which sets forth the clauses to be used in certain DOE contracts.

a. 48 CFR 952.204-2 , *Security Requirements*, which establishes the contractor's responsibility to protect classified information in contracts for research assistance, for ownership and operation of production facilities, or for performance which involves or is likely to involve classified information.

b. 48 CFR 952.204-70, *Classification/Declassification*, which establishes the contractor's responsibility to comply with DOE directives on classification and declassification in contracts for performance which involves or is likely to involve classified information.

c. 48 CFR 952.204-72, *Disclosure of Information*, a clause which must be used in place of 48 CFR 952.204-2 and 952.204-70 in certain contracts with educational institutions that are not likely to produce classified information to establish what must be done if classified information becomes involved in the contract.

7. DoD 5220.22-M, *National Industrial Security Program Operating Manual,* January 1995, as amended, which establishes requirements for classified information created by or in the possession of contractors, licensees, or permit holders.

   a. Chapter 4, *Classification and Marking,* Section 2, *Marking Requirements,* which details marking requirements for classified material.

   b. Chapter 5, *Safeguarding Classified Information.*

      (1) Section 1, *General Safeguarding Requirements,* which details requirements related to classified information for oral discussions, security checks, perimeter controls, and emergency procedures.

      (2) Section 2, *Control and Accountability,* which details requirements related to classified material for transmission records, accountability of Top Secret, receipt procedures, and working paper procedures.

      (3) Section 3, *Storage and Storage Equipment,* which describes the physical protection requirements for classified material.

      (4) Section 4, *Transmission,* which details how to transmit classified material.

      (5) Section 5, *Disclosure,* which details requirements for ensuring that classified information is disclosed only to authorized persons.

      (6) Section 6, *Reproduction,* which details requirements for controlling reproduction of classified material, marking copies, and accounting for Top Secret reproductions.

      (7) Section 7, *Disposition and Retention,* which requires disposition of classified material when no longer needed by return or destruction, and compliance procedures if classified material is retained after contract completion.

   c. Chapter 6, *Visits and Meetings,* which details requirements when it is anticipated that classified information will be disclosed during a visit to a cleared Federal or contractor facility or during a meeting of any type.

   d. Chapter 7, *Subcontracting,* which states the requirements and responsibilities of a contractor when disclosing classified information to a subcontractor.

   e. Chapter 9, *Special Requirements.*

      (1) Section 1, *Restricted Data and Formerly Restricted Data,* which details the requirements related to these classification categories.

      (2) Section 2, *DoD Critical Nuclear Weapon Design Information,* which details the requirements related to CNWDI.

f. Chapter 10, *International Security Requirements,* which provides requirements for control of classified information in international programs.

8. DOE O 241.1A, *Scientific and Technical Information Management,* 4-9-01, which establishes requirements and responsibilities to ensure access to classified and unclassified controlled scientific and technical information is controlled in accordance with legal or DOE requirements.

9. DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3-11-04, which establishes responsibilities and requirements for controlling access to and disseminating Sigma 14 and 15 nuclear weapon data (NWD).

10. DOE M 475.1-1A, *Identifying Classified Information,* 2-26-01, which provides requirements for managing the DOE classification and declassification program, including details for classifying and declassifying information, documents, and material.

11. DOE 5610.2, *Control of Weapon Data*, 8-1-80, which establishes responsibilities and requirements for controlling weapon data.

12. NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U),* 12-22-93 (a classified Naval Sea Systems Command Instruction under the control of the Assistant Administrator for Naval Reactors) which provides protection requirements for classified and unclassified NNPI.

13. NDP-1, *National Policies and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, (a classified document under the control of the Department of Defense, referred to as "National Disclosure Policy"), which provides guidance for dissemination of classified information to foreign governments.

Section B – Operations Security

1. National Security Decision Directive 298, *National Operations Security Program,*

1-22-88, which describes the OPSEC Program's objectives, requirements, and responsibilities.

Section C – Special Access Programs

1. 50 U.S.C. 2426, *Congressional Oversight of Special Access Programs,* which requires reports to Congress on SAPs and new SAPs annually and on changes in classification of SAPs and SAP designation requirements as they occur, unless the requirements are waived, and requires delays in initiating SAPs until 30 days after Congress has been notified.

2. Executive Orders (E.O.) and Presidential Directives, Office of the President.

a. E.O.12333, *United States Intelligence Activities,* 12-4-81, as amended by E.O. 13284, 1-23-03, and E.O. 13355, 8-27-04, which describes the goals, direction, duties, and responsibilities of the national intelligence effort.

b. E.O.12863, *President's Foreign Intelligence Advisory Board,* 9-13-93, as amended by E.O. 13070, 12-15-97, and E.O. 13301, 5-14-03, which establishes PFIAB to provide assessments of intelligence and the Intelligence Oversight Board as a standing committee of PFIAB to provide oversight of intelligence activities.

c. E.O. 12958, Classified National Security Information, as amended (see E.O. 13292, 3-25-03), Section 4.3, Special Access Programs.

(1) Section 4.3.(a), *Establishment of Special Access Programs,* establishes the standards for creating a SAP.

(2) Section 4.3.(b), *Requirements and Limitations,* limits the number given access to a SAP and requires a records system, oversight, annual review, and Presidential staff interface.

d. E.O.12968, *Access to Classified Information,* which establishes the Federal personnel security program.

(1) Section 2.2., *Level of Access Approval,* establishes in subsection (b) the standards for granting access to SAP-related classified information.

(2) Section 2.4, *Reciprocal Acceptance of Access Eligibility Determinations,* in subsection (c) authorizes agencies to establish additional investigative or adjudicative procedures for access to SAPs.

e. National Security Decision Directive (NSDD) 19, *Protection of Classified National Security Council and Intelligence Information,* which sets the requirements for protecting such information.

f. NSDD-84, *Safeguarding National Security Information,* 3-11-83, which requires signing a nondisclosure agreement before being granted access to Sensitive Compartmented Information.

3. Director of Central Intelligence (DCI) Directives (DCID).

a. DCID 1/7, *Security Controls on the Dissemination of Intelligence Information,* 6-30-98, which establishes policies, controls, and procedures for the dissemination and use of intelligence information.

b. DCID 1/19, *Security Policy for Sensitive Compartmented Information and Security Policy Manual,* 3-1-1995, which establishes policies and procedures for the security, dissemination, and use of SCI.

c. DCID 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)*, 12-29-91, which establishes the minimum policy concerning assignment and travel of Federal civilian, military, contractor, and consultant personnel who have, or who have had, access to SCI.

d. DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, 6-5-99, which establishes requirements for protecting SCI in automated information systems.

e. DCID 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, 7-2-98, which establishes standards, procedures, and security programs for the protection of SCI.

f. DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*, 7-11-01, which establishes policies, controls, and procedures for the dissemination and use of intelligence information and materials bearing DCI authorized control markings.

g. DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)*, 11-18-02 with administrative correction 12-23-02, which establishes SCIF physical security standards.

4. 32 CFR 2001.48, *Special Access Programs*, which is from the Information Security Oversight Office's (ISOO) *Classified National Security Information Directive Number 1*, 9-22-03.

a. 32 CFR 2001.48(a), *General*, requires enhanced controls for the protection of SAP information based on value, criticality, and vulnerability.

b. 32 CFR 2001.48(b), *Significant Interagency Support Requirements*, requires memoranda of agreement or understanding for SAPs with significant interagency support requirements.

5. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, as amended, which establishes requirements in Chapter 9, Section 3, for intelligence information created by or in the possession of contractors, licensees, or permit holders.

a. Section 9-301, *Definitions*, which defines pertinent terms.

b. Section 9-303, *Control Markings Authorized for Intelligence Information*, which details six markings and their use.

c. Section 9-304, *Limitation on Dissemination of Intelligence Information*, which requires written authorization of the releasing agency.

d. Section 9-305, *Safeguarding Intelligence Information,* which requires compliance with NISPOM classified material protection requirements, special instructions received from the Government, and compliance with restrictive markings.

e. Section 9-305, *Inquiries,* which requires inquiries to be referred to the releasing agency.

6. DoD 5220.22-M-Sup 1, *National Industrial Security Program Operating Manual Operating Manual Supplement,* February 1995, as amended, which establishes enhanced security requirements for Special Access Programs and Sensitive Compartmented Information.

7. Security Policy Board directives.

a. SPB Issuance 4-97, *National Policy on Reciprocity of Use and Inspection of Facilities,* 9-16-97.

b. SPB Issuance 5-97, *Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspection of Facilities,* 9-16-97.

8. DOE 5639.8A, *Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities,* 7-23-93, which establishes responsibilities and requirements for the protection of Foreign Intelligence Information and Sensitive Compartmented Information Facilities.

9. DOE 5670.1A, *Management and Control of Foreign Intelligence,* 1-15-92, which sets the responsibilities and requirements for managing foreign intelligence activities.

10. *DOE Sensitive Compartmented Information Facility Procedural Guide,* Office of Intelligence, 2-22-00, which implements the appropriate portions of the DCIDs.

Section D – Unclassified Controlled Information

1. United States Code (U.S.C.).

a. 5 U.S.C. 552, *The Freedom of Information Act,* as amended, which requires Federal agencies to make information available upon request by anyone, subject to certain exemptions and exceptions.

b. 5 U.S.C. 552a, *The Privacy Act of 1974,* as amended, which limits Federal agencies on establishing and releasing records on individuals and granting access to such records, and establishes certain rights concerning one's records.

c. 42 U.S.C. 2168 (Section 148, as amended, of the *Atomic Energy Act of 1954*), *Prohibition Against the Dissemination of Certain Unclassified Information,* which requires the Secretary of Energy to publish regulations protecting certain unclassified facility design information, physical protection information, and nuclear weapon or component information, and establishes civil and criminal penalties.

2. Title 10, Code of Federal Regulations (CFR), *Energy*.

   a. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*, which implements 42 U.S.C. 2168 by providing for the review of information, criteria for determining what is UCNI, physical protection standards, access requirements, and penalties for violations.

   b. 10 CFR, Part 1044, *Security Requirements for Protected Disclosures under Section 3164 of the National Defense Authorization Act for Fiscal Year 2000*, which sets requirements for the protected disclosure of Unclassified Controlled Nuclear Information under the whistleblower protection granted by Section 3164.

3. Executive Order 13222, *Continuation of Export Control Regulations*, 8-17-01, which authorizes, to the extent lawful, the enforcement of the *Export Administration Act of 1979*, which has lapsed, and the *Export Administration Regulations*, which were originally issued to implement the Act.

4. 15 CFR Chapter VII, Subchapter C (Parts 730 through 774), *Export Administration Regulations*, which implement Executive Order 13222 and other legal authorities to control the export and re-export of certain articles, services, and unclassified technical information.

5. 22 CFR Chapter I, Subchapter M (Parts 120 through 130), *International Traffic in Arms Regulations*, which implement the *Arms Export Control Act*, 22 U.S.C. 2778, which authorizes the Department of State to control the export and import of certain defense articles, services, and unclassified technical information.

6. 32 CFR 250, *Withholding of Unclassified Technical Data from Public Disclosure*, which implements 10 U.S.C. 130 requirements to protect sensitive unclassified information belonging to the Department of Defense and having a space or military application, including Naval Nuclear Propulsion Information.

7. 48 CFR 952.204 (DEAR 952.204), *Clauses Related to Administrative Matters*, which sets forth the clauses to be used in certain DOE contracts.

   a. 48 CFR 952.204–71, *Sensitive Foreign Nation Controls*, a clause which must be used in unclassified research contracts which may involve making unclassified information about nuclear technology available to certain sensitive foreign nations.

   b. 48 CFR 952.204-72, *Disclosure of Information*, a clause which must be used in place of 48 CFR 952.204-2 and 952.204-70 in certain contracts with educational institutions that are not likely to produce classified information to establish what must be done if classified information becomes involved in the contract.

8. DOE O 241.1A, *Scientific and Technical Information Management*, 4-9-01, which establishes requirements and responsibilities to ensure access to unclassified controlled scientific and technical information is controlled in accordance with legal or DOE requirements.

9. DOE O 471.1-1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 6-30-00, which establishes responsibilities for the protection of UCNI.

10. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, 4-9-03, which establishes responsibilities for the protection of OUO information.

11. DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, 6-30-00, which establishes requirements for the protection of UCNI.

12. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, 4-9-03, which establishes requirements for the protection of OUO information.

13. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, 4-9-03, which provides guidance for implementing DOE O 471.3 and DOE M 471.3-1.

Section E – Technical Surveillance Countermeasures Program

1. Executive Orders (E.O.) and Presidential Directives, Office of the President.

   a. E.O. 12333, *United States Intelligence Activities* (with classified attachment), 4-12-81, which provides policies for electronic surveillance countermeasures.

   b. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, 7-5-90, which provides objectives, policies, and an organizational structure for national activities for protecting systems which possess or communicate sensitive information from hostile exploitation.

   c. Presidential Decision Directive/NSC-61, *U.S. Department of Energy Counterintelligence Program*, February 1998, which, in addition to DOE counterintelligence provisions, requires each agency to determine the need for a TSCM program and the standards for such programs.

2. Director of Central Intelligence Directives (DCID).

   a. DCID 6/2, *Technical Surveillance Countermeasures*, 3-11-99, which establishes requirements and procedures for the conduct and coordination of technical surveillance countermeasures.

   b. DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, 6-5-99, which establishes requirements for protecting intelligence information in automated information systems.

3. 32 CFR Part 2001, Classified National Security Information, which is the Information Security Oversight Office's (ISOO) *Classified National Security Information Directive Number 1*, 9-22-03.

   a. 32 CFR 2001.49, *Telecommunications and Automated Information Systems and Network Security*, requires compliance with national policy issuances identified in

the *Index of National Security Telecommunications and Information Systems Security Issuances* and in DCID 6/3.

b. 32 CFR 2001.50, *Technical Security*, requires a determination of whether technical countermeasures are needed to protect classified information.

4. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, as amended, which establishes requirements for classified information created by or in the possession of contractors, licensees, or permit holders. Chapter 11, *Miscellaneous Information,* Section 1, *Tempest*.

a. Section 11-101, *TEMPEST Requirements,* which requires Government direction before investigating or studying compromising emanations and before imposing TEMPEST countermeasures on subcontractors.

b. Section 11-102, *Cost*, which addresses costs of TEMPEST countermeasures.

5. Security Policy Board directives.

a. SPB Issuance 6-97, *National Policy on Technical Surveillance Countermeasures,* 9-16-97.

b. Procedural Guide No. 1, *Conduct of a Technical Surveillance Countermeasures Survey,* 3-24-99.

c. Procedural Guide No. 2, *Requirements for Reporting and Testing Technical Surveillance Penetrations*, 3-24-99.

d. Procedural Guide No. 3, *Requirements for Reporting and Testing Technical Hazards,* 3-24-99.

6. Telephone Security Group (TSG) Standards, national standards available from secure websites (Joint Worldwide Intelligence Communications System (JWICS) at http://www.iccio.ic.gov/SECURITYtob.asp or SIPRNET at http://www.tscm.inscom.army.smil.mil/regs.htm.

a. TSG No. 1, *Introduction to Telephone Security*.

b. TSG No. 2, *Guidelines for Computerized Telephone Systems*.

c. TSG No. 3, *Type-Acceptance Program for Telephones Used with the Conventional Central Office Interface*.

d. TSG No. 4, *Type-Acceptance Program for Electronic Telephones Used in Computerized Telephone Systems*.

e. TSG No.5, *On-Hook Telephone Audio Security Performance Specifications*.

f. TSG No.6, *Telephone Security Group Approved Equipment*.

g. TSG No. 7, *Telephone Security Group Guidelines for Cellular Telephones*.

h. TSG No. 8, *Microphonic Response Criteria for Noncommunications Devices*.

7. National Security Telecommunications and Information Systems Security Issuance 7000 (NSTISSI 7000), *Tempest Countermeasures for Facilities.*

8. DOE M 200.1-1, *Telecommunications Security Manual*, 3-1-97, which establishes a Communications Security program, including protection of crypto facilities.

9. DOE 1450.4, *Consensual Listening-in to or Recording Telephone/Radio Conversations*, 11-12-92, which sets the policy, responsibilities, and procedures for listening or recording telephone or radio conversations.

DOE M 470.4-5, *Personnel Security*

1. United States Code (U.S.C.).

a. 5 U.S.C. 552a, *The Privacy Act of 1974*, which sets conditions for disclosures of records maintained on individuals and penalties for wrongful disclosures.

b. 21 U.S.C. 802, *Controlled Substances Act of 1970*, which defines illegal drugs.

c. 42 U.S.C. 2011 *et seq*. [*Atomic Energy Act of 1954 (AEA)*, as amended].

(1) 42 U.S.C. 2161 (Section 141, *AEA*), which establishes the policy to control the dissemination and declassification of Restricted Data.

(2) 42 U.S.C. 2163 (Section 143, as amended, *AEA*), which authorizes cleared DOE and contractor employees to allow cleared DoD and contractor employees access to Restricted Data.

(3) 42 U.S.C. 2165 (Section 145, as amended, *AEA*), which establishes rules for access to Restricted Data that contractors or licenses must agree not to grant access to unauthorized personnel; that OPM or another Federal agency shall investigate and a favorable determination shall be made before DOE personnel are granted access; that the FBI shall investigate if there is a questionable loyalty issue, if the President instructs, or if position is of high degree of importance or sensitivity; r agency investigative reports may be accepted; that DOE makes the access determinations; and that access may be granted during time of war or national emergency before the investigation is completed.

(4) 42 U.S.C. 2201(b) (Section 161b, as amended, *AEA*), which authorizes DOE to set standards governing possession and use of special nuclear material.

2. Executive Orders (E.O.) and Presidential Directives, Office of the President.

a. E.O. 10450, *Security Requirements for Government Employees*, 4-27-53, as amended, which establishes the requirements for determining that all Federal employees are loyal, reliable, trustworthy, and of good conduct and character.

b. E.O. 10865, *Safeguarding Classified Information within Industry*, 2-20-60, as amended, which establishes the basis for the industrial security program for cleared civilian personnel.

c. E.O. 12829, *National Industrial Security Program*, 1-6-93, as amended, by E.O. 12885, 12-14-93, which prescribes requirements to prevent unauthorized disclosure of classified information released by Federal agencies to their contractors.

d. E.O.12968, *Access to Classified Information*, which establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

e. National Security Directive (NSD) 63, *Single Scope Background Investigations*, 10-21-01, which describes minimum investigative scopes and standards to be adopted by all Federal agencies for access for collateral, top secret National Security Information, and Sensitive Compartmented Information

3. National Security Advisor memo, *Implementation of Executive Order 12968*, 3-24-98, with attachments *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* and *Investigative Standards for Background Investigations for Access to Classified Information.*

4. Director of Central Intelligence Directive (DCID) No. 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, 7-2-98.

5. Federal Investigations Notice No. 95-5, *Executive Order 12968, National Security Directive 63 and Standard Form 86*, Office of Personnel Management, 10-3-95.

6. Title 5, Code of Federal Regulations (CFR), *Administrative Personnel*.

a. 5 CFR 732, *National Security Positions*, which implements E.O. 10450 throughout the Federal agencies.

b. 5 CFR 736, *Personnel Investigations*, which specifies requirements for personnel investigations conducted by the Office of Personnel Management (OPM), and for those conducted under delegated authority from OPM.

7. Title 10, CFR, *Energy*.

a. 10 CFR Part 707, *Workplace Substance Abuse Programs at DOE Sites*, which establishes procedures for drug testing in DOE.

b. 10 CFR Part 712, *Human Reliability Program*, which consolidates the old Personnel Security Assurance Program (PSAP) and the old Personnel Assurance Program (PAP) into a single program and establishes procedures for the resulting new program.

c. 10 CFR Part 725, *Permits for Access to Restricted Data*, which establishes procedures and standards for the issuance of Access Permits.

d. 10 CFR Part 1008, *Records Maintained on Individuals (Privacy Act)*, which establishes the procedures to implement the Privacy Act of 1974 within DOE.

e. 10 CFR Part1016, *Safeguarding of Restricted Data*, which establishes requirements for protecting Restricted Data received or developed under an access permit.

8. Title 48, CFR, *Federal Acquisition Regulations System*, Chapter 9, *Department of Energy* [Acquisition Regulations (DEAR)].

a. 48 CFR 952.204-2, *Security Requirements*, which prescribes contract clauses that contain rules for contractors to protect classified information and SNM.

b. 48 CFR 952.204-73, *Facility Clearance*, which is a solicitation provision required when the resulting contract or subcontract will require employees to hold access authorizations.

c. 48 CFR 970.2201, *Basic Labor Policies*, which establishes employment standards for management and operating contractors, including pre-employment check requirements.

d. 48 CFR 970.5204-2, *Laws, Regulations and DOE Directives*, which details requirements a site/facility management contractors must comply with.

9. DOE 3731.1, *Suitability, Position Sensitivity Designations, and Related Personnel Matters*, 12-19-89, which set responsibilities and requirements for suitability investigations and determinations, and addresses the interrelationship between suitability and access authorization.

10. *CPCI User Guide*, August 2000, Office of Personnel Security (SO-30.2), which establishes for system users the system requirements, operations, and data input procedures for the Central Personnel Clearance Index and other system components.

DOE M 470.4-6, *Nuclear Material Control and Accountability*

1. Title 42, United States Code (U.S.C.), Section 2011 *et seq*. [*Atomic Energy Act of 1954 (AEA)*, as amended]; specifically, the following sections:

a. 42 U.S.C. 2073 (Section 53, as amended, *AEA*), Domestic *Distribution of Special Nuclear Material*, which describes the licensing process used by the NRC for the transfer and receipt of nuclear material subject to licensing within the U.S.

b. 42 U.S.C. 2074 (Section 54, as amended, *AEA*), *Foreign Distribution of Special Nuclear Material*, which describes the licensing process used by the NRC for the transfer and receipt of nuclear material subject to licensing with foreign nations.

c. 42 U.S.C. 2077 (Section 57, as amended, *AEA*), *Unauthorized Dealings in Special Nuclear Material*, which details restrictions on the trafficking of special nuclear material, including unauthorized production or shipment of special nuclear material.

d. 42 U.S.C. 2094 (Section 64, as amended, *AEA*), *Foreign Distribution of Source Material*, which provides for distribution of source material.

e. 42 U.S.C. 2095 (Section 65, *AEA*), *Reports*, which authorizes DOE to issue regulations and orders requiring reports of ownership, possession, extraction, refining, shipment, or other handling of source material.

f. 42 U.S.C. 2112 (Section 82, *AEA*), *Foreign Distribution of Byproduct Material*, which provides for the distribution of byproduct material.

g. 42 U.S.C. 2121 (Section 91, as amended, *AEA*), *Authority of Commission*, which provides the reasons/authorities for transferring special nuclear material, including weapons, pursuant to presidential directive.

h. 42 U.S.C. 2133 (Section 103, as amended, *AEA*), *Commercial Licenses*, which provides conditions under which an individual may apply and be granted, by the NRC, a license for the possession and transfer of nuclear material.

i. 42 U.S.C. 2134 (Section 104, as amended, *AEA*), *Medical, Industrial, and Commercial License*, which provides rules for licensing the use of nuclear material in commercial settings.

j. 42 U.S.C. 2153 (Section 123, as amended, *AEA*), *Cooperation with Other Nations*, which provides for cooperation regarding exchanges of nuclear material between the United States and other nations.

k. 42 U.S.C. 2164 (Section 144, as amended, *AEA*), *International Cooperation*, which provides for cooperation regarding data exchange that involves sensitive nuclear information between the U.S. and foreign nations.

2. *Agreement Between the United States of America and the IAEA for the Application of Safeguards in the United States*, and *Additional Protocol*, which supports the *Treaty on the Nonproliferation of Nuclear Weapons*, and provides for the application of International Atomic Energy Agency (IAEA) safeguards to nuclear materials in facilities in the U.S. not associated with activities of direct national security significance. Copies are available from the U.S. Government Printing Office.

3. IAEA Information Circular 207 (INFCIRC/207), *Notification to the Agency [IAEA] of Exports and Imports of Nuclear Material*, 7-26-74, and amendment letter, 9-15-82, which requests that the U.S. report exports and imports of quantities of nuclear materials. Copies are available from the Office of Arms Control and Nonproliferation (NA-24) or the IAEA.

4. Office of Management and Budget (OMB) Circular A-130, Revision 4, *Management of Federal Information Resources*, 11-6-03, which establishes policy for the management of Federal information resources, including procedural and analytical guidelines for implementing specific aspects of these policies.

5. Title 10, Code of Federal Regulations (CFR), *Energy*.

a. 10 CFR, Chapter I, *Nuclear Regulatory Commission*, which contains the regulations

applicable to NRC and NRC agreement State licensees involved in activities concerning nuclear materials not subject to DOE requirements, including 10 CFR Part 74, *Material Control and Accounting of Special Nuclear Material.*

b. 10 CFR Part 830, *Nuclear Safety Management*, which contains nuclear safety and quality assurance requirements.

c. 10 CFR Part 835, *Occupational Radiation Protection*, which provides guidance on sealed radioactive source control (10 CFR 835.1201) and accountable sealed radioactive source control (10 CFR 835.1202).

6. DOE O 142.2, *Safeguards Agreement and Protocol with the International Atomic Energy Agency*, 1-7-04, which prescribes requirements and responsibilities for compliance with the agreement and protocol between the Government and the International Atomic Energy Agency for the safeguards application in the United States.

7. DOE O 151.1B, *Comprehensive Emergency Management System*, 10-29-03, which establishes requirements and responsibilities for emergency planning, preparedness, readiness assurance, response, and recovery operations.

8. DOE O 413.1A, *Management Control Program*, 4-18-02, which requires evaluation and reporting on the status of the management controls in DOE's programs and administrative functions, and reporting on corrections of problems identified.

9. DOE O 420.1A, *Facility Safety*, 5-20-02, which establishes facility safety requirements.

10. DOE M 435.1-1, *Radioactive Waste Management Manual*, 6-19-01, which describes requirements and specific responsibilities for the management of high level, transuranic, and low-level wastes and the radioactive component of mixed waste.

11. DOE G 441.1-13, *Sealed Radioactive Source Accountability and Control Guide*, 4-15-99, which describes an acceptable methodology for establishing and operating a sealed radioactive source accountability and control program that will comply with 10 CFR 835.

12. DOE O 450.1, *Environmental Protection Program*, 1-15-03, which establishes the Environmental Protection Program for DOE operations.

13. DOE O 461.1A, *Packaging and Transfer or Transportation of Materials of National Security Interest*, 4-26-04, which establishes requirements and responsibilities for the Transportation Safeguards System packaging and transportation and onsite transfer of nuclear explosives, nuclear components, Naval fuel elements, Category I and -II special nuclear materials, special assemblies, and other materials of national security interest.

14. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, 4-9-03, which lists FOIA exemption categories.

15. DOE 5480.20A, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities*, 11-15-94, which establishes the requirements for contractor personnel involved in the operation, maintenance, and technical support of DOE-owned reactors and nonreactor nuclear facilities.

16. *Reporting Identification Symbol (RIS) Directories*, Nuclear Materials Management and Safeguards System (NMMSS), which contain lists of valid RISs for DOE and NRC nuclear facilities, Department of Defense facilities, Mutual Defense facilities, foreign facilities, and specific organizations. For domestic facilities, these documents list the names, addresses, and telephone numbers of the facilities, and any special requirements for notification concerning shipment of nuclear material. For international facilities, the IAEA facility codes and country codes are listed. Copies are available from the NMMSS operator.

17. *International Nuclear Materials Tracking System (INMTS) Data Entry Procedures*, DOE Office of Plutonium, Uranium and Special Materials Inventory, which provides for the preparation and submission of information concerning U.S.-supplied nuclear materials in foreign countries in which the U.S. has an interest.

18. U.S. Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response, Washington, DC 20555-0001.

    a. NUREG/BR-0006, Revision 6, *Instructions for Completing Nuclear Material Transaction Reports (DOE/NRC Forms 741 and 740M)*, 10-1-03, which is a brochure for use by facilities licensed by the NRC when reporting shipments, receipt, and inventory adjustments of nuclear material that is not Government-owned and located at a licensee facility.

    b. NUREG/BR-0007, Revision 5, *Instructions for the Preparation and Distribution of Material Status Reports (DOE/NRC Forms 742 and 742C)*, 10-1-03, which is a brochure for use by facilities licensed by the NRC to possess certain special nuclear material when reporting receipt, production, possession, transference, consumption, disposal, and loss.

19. *Nuclear Wallet Cards*, 6th edition, January 2000, National Nuclear Data Center, Brookhaven National Laboratory, Upton, New York, which are the source documents for nuclear material properties including radioactive decay constants. (Available online at www.nndc.bnl.gov.)

20. ANSI Standards, American National Standards Institute, Inc., 25 West 43rd Street, 4th Floor, New York, NY 10036.

    a. ANSI N15.1, *Classification of Unirradiated Uranium Scrap*, 1970.

    b. ANSI N15.10, *Classification of Unirradiated Plutonium Scrap*, 1987.

c. ANSI N15.18, *Nuclear Materials – Mass Calibration Techniques for Control*, 1988.

d. ANSI N15.19, *Nuclear Material Control – Volume Calibration Techniques*, 1989.

e. ANSI N15.28, *Nuclear Materials Control – Guide for Qualification and Certification of Safeguards and Security Personnel*, 1991.

f. ANSI N15.36, *Nuclear Materials – Nondestructive Assay Measurement Control and Assurance*, 1994.

g. ANSI N15.41, *Derivation of Measurement Control Programs – General Principles*, 1994.

h. ANSI N15.51, *Nuclear Materials Management – Measurement Control Program – Nuclear Materials Analytical Chemistry Laboratory*, 1996.

i. ANSI N15.54, *Instrumentation – Radiometric Calorimeters Measurement Control Program*, 1991.

21. ASTM Standards, ASTM International, 100 Barr Harbor Drive, PO Box C700, Conshohocken, PA 19428-2959.

a. ASTM C993-97(2003), *Standard Guide for In-Plant Performance Evaluation of Automatic Pedestrian SNM Monitors*, 2003.

b. ASTM C1112-99, *Standard Guide for Application of Radiation Monitors to the Control and Physical Security of Special Nuclear Material*, 1999.

c. ASTM C1215-92(1997), *Standard Guide for Preparing and Interpreting Precision and Bias Statements in Test Method Standards Used in the Nuclear Industry*, 1997.

d. ASTM C1169-97(2003), *Standard Guide for Laboratory Evaluation of Automatic Pedestrian SNM Monitor Performance*, 2003.

e. ASTM C1189-02, *Standard Guide to Procedures for Calibrating Automatic Pedestrian SNM Monitors*, 2002.

f. ASTM C1236-99, *Standard Guide for In-Plant Performance Evaluation of Automatic Vehicle SNM Monitors*, 1999.

g. ASTM C1237-99, *Standard Guide to In-Plant Performance Evaluation of Hand-Held SNM Monitors*, 1999