DOE M 470.4-7

Approved: 08-26-05
Review: 08-26-07

SAFEGUARDS AND SECURITY PROGRAM REFERENCES

U.S. DEPARTMENT OF ENERGY

Office of Security and Safety Performance Assurance

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

SAFEGUARDS AND SECURITY PROGRAM REFERENCES

1. PURPOSE. This Manual establishes definitions for terms related to the Department of Energy (DOE) Safeguards and Security (S&S) Program. This Manual also contains lists of references and acronyms/abbreviations applicable to S&S Program directives.

2. OBJECTIVES.

   a. To establish definitions for S&S Program terms.

   b. To establish a comprehensive list of references and acronyms/abbreviations applicable to S&S Program directives.

3. CANCELLATION. The *Safeguards and Security Glossary of Terms*, dated 12-18-95 is canceled. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with the directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled directives.

4. APPLICABILITY.

   a. Departmental Elements. Except for the exclusion in paragraph 4.b., this Manual applies to all Departmental Elements listed on Attachment 1, including National Nuclear Security Administration (NNSA). This Manual automatically applies to Departmental Elements created after it is issued.

   b. Exclusion. Consistent with the responsibilities identified in Executive Order 12344 (as prescribed by 42 U.S.C. 7158), the Deputy Administrator for Naval Reactors will determine the applicability of this Manual for activities and facilities under his control.

5. CONTACT. Questions concerning this Manual should be directed to the Office of Security at (301) 903-4803.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTENTS

SECTION A – SAFEGUARDS AND SECURITY GLOSSARY

The *Safeguards and Security Glossary* contains DOE safeguards and security (S&S) program terms and definitions. These terms and their definitions reflect the latest additions and changes to terminology commonly used in S&S programs. Generally used terms defined in most dictionaries have been intentionally omitted from the Glossary.

Although a Manual including the *Safeguards and Security Glossary* would be considered a requirements document, it is not intended that the definitions imply or be construed as establishing DOE requirements. Therefore, if the definition of a term in the Glossary should differ from an analogous one in a programmatic manual, the definition in the programmatic manual will take precedence.

Recommendations for revisions to this Glossary are encouraged and should be submitted to the Office of Security for consideration in developing future revisions.

A

"A" MATERIALS. Special nuclear material in Attractiveness Level A. This includes nuclear material contained in weapons and test devices. Partially assembled nuclear weapons and test devices also may be included in this attractiveness level if assembly of an improvised nuclear device can be completed using commercially available materials. All "A" materials are Category I.

ABRUPT LOSS. A loss occurring in the time interval between consecutive sequential performances of a material control test which is designed to detect anomalies potentially indicative of a loss of strategic special nuclear material from a specific unit of strategic special nuclear material (i.e., a quantity characterized by a unique measurement) introduced into a process. (10 CFR 74.4, *Definitions*)

ABRUPT THEFT OR DIVERSION. A theft or diversion that is accomplished during a single occurrence.

ACCEPTED RISK. The acknowledgment that a protection system may not achieve 100 percent protection against all occurrences, but further improvement in the system is not justified, and that the Department is willing to accept the potential consequences of an adversarial act.

ACCESS. Refers to any of the following.

1. The knowledge, use, or possession of classified or unclassified controlled information required by an individual to perform official duties that is provided to the individual on a need-to-know basis. (Information Security)
2. The ability and opportunity to obtain knowledge of classified information. (National Industrial Security Program Operating Manual)
3. Situations that may provide an individual proximity to or control over special nuclear material. (Physical Protection/Nuclear Material Control & Accountability)
4. The proximity to a nuclear weapon and/or special nuclear material in such a manner as to allow the opportunity to divert, steal, tamper with, and/or damage the weapon or material. (Physical Protection/Nuclear Material Control & Accountability)
5. Ability and means to communicate with (i.e., provide input to or receive output from), or otherwise make use of any information, resource, or component in a classified automated information system. (Cyber Security)
6. Ability to enter a defined area. (Physical Protection)
7. The mode of a sensor or alarm group during which the physical sensor states of "OK" and "detect" are hidden from the operator, but "tamper" is not. (Physical Protection)

ACCESS AUTHORIZATION. An administrative determination that an individual is eligible for access to classified matter when required by official duties or is eligible for access to, or control over, special nuclear material.

ACCESS AUTHORIZATION EXTENSION. The process that allows an individual to have concurrent active DOE access authorizations under the cognizance of two or more Departmental Elements, two or more employers, or one employer under two or more contract numbers.

ACCESS AUTHORIZATION TRANSFER. The process that simultaneously allows an individual's DOE access authorization to be terminated at one processing personnel security office and granted at another processing personnel security office.

ACCESS CONTROL. The process of permitting access or denying access to information, facilities, nuclear materials, resources, or designated security areas.

ACCESS CONTROL MEASURES. Hardware and software features, physical controls, operating procedures, administrative procedures, and various combinations of these designed to detect or prevent unauthorized access to classified information; special nuclear materials; Government property; automated information systems, facilities, or materials; or areas containing the above and to enforce use of these measures to protect Departmental security and property interests.

ACCESS PERMIT. An authorization, issued by the Department in accordance with 10 CFR 725, *Permits for Access to Restricted Data*, which affords access by a specifically named person or organization (permittee) to Restricted Data applicable to the civilian uses of atomic energy in accordance with terms and conditions stated on the permit.

ACCESS PERMITTEE. An individual or organization that has been issued an access permit by the Department providing access to Restricted Data applicable to civilian uses of nuclear energy in accordance with the terms and conditions stated on the permit and with security regulations in 10 CFR 725, *Permits for Access to Restricted Data*.

ACCOUNTABLE CLASSIFIED REMOVABLE ELECTRONIC MEDIA (ACREM). Classified Removable Electronic Media (CREM) containing Secret/Restricted Data (S/RD) or higher classification, or containing any Sigma 1, 2, 14, or 15 or a combination of nuclear weapons design/testing data.

ACCOUNTABILITY.

1. That part of the Materials Control and Accountability program which employs physical inventories, measurements, accounting records, and reports to account for nuclear materials. (See also NUCLEAR MATERIALS ACCOUNTABILITY.)
2. A system which provides auditable control measures associated with classified matter through the use of a verifiable inventory and the establishment of a custodial chain.

ACCOUNTABILITY MEASUREMENT. A quantitative measurement of the amount of nuclear material in an item or location made to establish initial book values for the material or to replace the existing book value with a more accurate measured value.

ACCREDITATION.

1. A DOE process to formally recognize S&S training programs and courses that have satisfied training objectives, standards, and criteria.
2. The formal acknowledgment (written or electronic) of the decision by the designated approval authority to authorize an automated information system to process, store, transfer, or provide access to classified automated information in a specific information system's security environment established by a specific classified automated information systems security plan.

ACCREDITATION LEVEL. The highest classification level and most restrictive classification category that a classified automated information system has been authorized to process.

ACCURACY. A measure of the agreement between the true or assigned value and the measured value. (Nuclear Material Control & Accountability)

ACOUSTIC SECURITY. Physical and technical security measures specifically designed and used to deny aural access to an area set apart for the discussion of unclassified controlled or classified information.

ACTIVATED BARRIER. Dispersible materials which are activated either remotely or in response to a stimulus, and which are designed for direct interference with human sensory and/or motor processes. They include non-pyrotechnic smoke, aqueous foam, rigid foam, cold smoke, and chloracetophenon (CN) gas.

ACTIVE INVENTORY.

1. Nuclear material contained within the material balance area that enters into calculation of the limit of error and control limit for the material balance area (e.g., items under tamper-indicating devices that were on both the beginning and ending inventories would not be included).
2. The sum of additions to inventory, beginning inventory, ending inventory, and removals from inventory, after all common terms have been excluded. Common terms are any material values which appear in the active inventory calculation more than once and come from the same measurement. (10 CFR 74.4, *Definitions*)

ACTIVE PROTECTION SYSTEM. A permissive action link (PAL) system that senses and responds to unauthorized intrusions with an appropriate penalty, usually weapon disablement.

ACTUAL INVENTORY DIFFERENCE. The portion of the *inventory difference* that is not *explained inventory difference*; expressed mathematically as:
Inventory difference (-) explained inventory difference = actual inventory difference.

ADJUSTMENT. An entry into the nuclear material accounting records to reflect an approved, justified, and documented change.

ADMINISTRATIVE CHECK. A review to determine that no irregularities appear to exist, no items are obviously missing, and no tampering is indicated.

ADMINISTRATIVE CONTROLS. Those provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure the secure operation of a facility.

ADVERSARY. Any government, organization, group, or individual whose interests are adverse to those of the U.S. Government in general and to those of the Department in particular.

ADVERSE INFORMATION / DEROGATORY INFORMATION.

1. Any factual and verifiable unfavorable information that creates a question as to an individual's eligibility for an access authorization or an entity's eligibility for a favorable Foreign Ownership, Control, or Influence determination. (See also DEROGATORY INFORMATION, and 10 CFR 710.8, *Criteria*.)
2. Any information that adversely reflects on the integrity or character of a cleared employee that suggests his or her ability to protect classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. (National Industrial Security Program Operating Manual)
3. Any information that adversely reflects on the ethics and compliance program of a company with a cleared facility that suggests the company's ability to protect classified information and/or special nuclear material may be impaired.

AGREEMENT FOR COOPERATION. Any agreement with another national or regional defense organization authorized or permitted by the Atomic Energy Act of 1954.

AGREEMENT STATE. Any state of the United States with which the U.S. Nuclear Regulatory Commission, or its predecessor, the Atomic Energy Commission, has entered into an agreement under 42 U.S.C. 2021 [Section 274, as amended, of the Atomic Energy Act of 1954].

ALARM ASSESSMENT. The process of determining an alarm condition stimulus.

ALARM CONDITION. A security event that must be reported to the console operator.

ALARM GROUP. Intrusion detection devices configured for a specific location and/or facility. It may consist of a selected number of door/gate contact switches (balanced magnetic switches), volumetric devices (passive infrared and/or microwave) or linear detector devices (infrared, ported coaxial, fence protection devices, taut-wire, electric-field, microwave), or a combination of detectors configured to pre-assigned zones or alarm points.

ALARM LIMIT. A control limit established for an inventory difference which, when exceeded, requires immediate action and reporting. (Alarm limits are generally established at the 99 percent confidence level.)

ALARM PROCESSING. The processing of information transmitted from devices (such as intrusion detection sensors, badge readers, and emergency sensors) interfaced to the system.

ALARM ZONE. A specified area that is protected by one or more intrusion detection devices.

ANNUNCIATOR. A visual or audible signaling device (monitor) that indicates the condition of associated circuits. Usually, this is accomplished by activation of a graphics display and audible sound.

ANTIJAMMING SYSTEM. Any system used to reduce the effectiveness of deliberate attempts to jam electromagnetic receivers.

APPARENT LOSS. The inability to physically locate or otherwise to account for any of the following.

1. Any identifiable or discrete item (e.g., batch, lot, or piece) containing nuclear material.
2. A nuclear material inventory difference in which the book inventory is larger than the physical inventory by an amount in excess of the established alarm limit.
3. A shipper/receiver difference involving a discrepancy in which fewer items were received than were shipped.
4. A shipper/receiver difference whose magnitude exceeds the combined limit of error for the shipment and for which the receiver measures less material than the shipper.

APPROVED SECURITY CONTAINER. A security file container, originally procured from a Federal Supply Schedule supplier, that conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers must be labeled "General Services Administration Approved Security Container" on the outside of the top drawer and have a lock meeting Federal Specification FF-L-2740, *Locks, Combination*.

ARMED ESCORT. An armed person, uniformed or plain-clothed, whose primary duty is to protect special nuclear material shipments against theft or radiological sabotage.

ARREST. Any act, including taking, seizing or detaining of a person, that indicates an intention to take a person into custody and that subjects the person to the control of the person making the arrest.

ASSAULTER. A certified Security Police Officer III capable of performing close-quarters battle, stronghold, emergency, and vehicle assault operations.

ASSESSMENT.

1. An evaluation of the effectiveness of an activity/operation or a determination of the extent of compliance with required procedures and practices. (S&S Program Planning and Management)
2. An evaluation of a Material Control and Accountability anomaly or Material Discrepancy Indicator. (Material Control Indicators)
3. An appraisal of the credibility, reliability, pertinence, accuracy, or usefulness of information. (S&S Program Planning and Management)
4. An evaluation of a physical security alarm. (Physical Protection)
5. Determination of the validity and priority of an incident. (S&S Program Planning and Management/Physical Protection)

ASSURANCE . A measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce security policy. (Cyber Security)

ASSURANCE TESTING. A process used to determine that the security features of a system are implemented and functioning as designed and that they are adequate for the proposed environment. NOTE: This process may include hands-on functional testing, penetration testing, and/or software verification.

ATOMAL. A North Atlantic Treaty Organization marking applied to (1) Restricted Data or Formerly Restricted Data provided by the United States to the North Atlantic Treaty Organization or (2) "U.K. Atomic Information" provided by the United Kingdom.

ATOM PERCENT. A measure of composition. As applied to isotopic composition, the fraction obtained by dividing the number of atoms of the isotope of interest by the total number of atoms of all isotopes present in the element, and multiplying by 100. May also be used to specify the fraction of an element in a compound or mixture (e.g., the atom percent of oxygen in UO_3).

ATTRACTIVENESS LEVEL. A categorization of nuclear material types and compositions that reflects the relative ease of processing and handling required to convert that material to a nuclear explosive device.

ATTRIBUTE MEASUREMENT. A measurement of some property of a defined group or population of items based on whether or not the items in a sample do or do not possess a given characteristic, or "attribute."

AUTHENTICATION. A security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's authorization to receive specific categories of information. (Information Security)

AUTHENTICATOR. Means used to confirm the identity or eligibility of a station, originator, or individual.

AUTHORIZATION. Access rights granted to a user, program, or process.

AUTHORIZED FIREARMS. Firearms approved by the Department and issued by the responsible Departmental authority or contractor to be used by protective force officers in the performance of duties.

AUTHORIZED INVESTIGATIVE AGENCY. An agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information. (Executive Order 12968, *Access to Classified Information*)

AUTOMATED ACCESS CONTROL SYSTEM. An electronic or electro-mechanical system used to allow authorized movement of personnel, vehicles, or material through entrances and exits of a secured area. Authorization is obtained by the user entering personal identification information (e.g., through a magnetic card reader, personal identification number, or biometric scan), an electronic comparison of identification data against an authorized users list, and activation of the portal unlock mechanism if the requestor's name is on the list of authorized personnel.

AUTOMATED INFORMATION SYSTEM SECURITY.

1. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in computer systems, as well as measures designed to prevent denial of authorized use of the system.
2. All security safeguards needed to provide an acceptable level of protection for automated information systems and the classified data processed. (National Industrial Security Program Operating Manual)

AUTOMATED SURVEILLANCE SYSTEM. A logically connected set of mechanized and/or electronic components that may be substituted for direct human observation. (Nuclear Material Control & Accountability)

AUTOMATIC DECLASSIFICATION. The declassification of matter based solely upon the occurrence of a specific date or event as determined by classification guidance or the expiration of a maximum time frame for duration of classification established under Executive Order 12958, *Classified National Security Information,* as amended.

B

"B" MATERIALS. Special nuclear material in Attractiveness Level B. Such material is metal which can be used in its existing form, or that can be used after simple mechanical removal of cladding, packaging, or matrix material, to produce a nuclear weapon or improvised nuclear device. Direct use of these materials in a nuclear device can be accomplished through casting, forming, or other non-chemical operations.

BACKGROUND INVESTIGATION. An official inquiry into the activities of a person designed to develop information from a review of the records, one or more interviews of the subject, and interviews of people having knowledge of the subject.

BALANCED MAGNETIC SWITCH. A device (magnetically operated switch), using a balanced magnetic field, designed to detect the opening of a secured door, window, or other point of entry. In addition, it detects attempts to defeat the switch by substituting a magnetic field and may have provisions for internal adjustments and detection of switch tampering attempts.

BARRIER. A coordinated series of natural or fabricated impediments that direct, restrict, limit, delay, or deny entry into a designated area.

BATCH. A particular portion or lot of nuclear material that is handled as a unit for accounting purposes and for which the composition and quantity are defined by a single set of specifications or measurements. The material may be in bulk form or contained in a number of separate items.

BATCH NAME/NUMBER. Under the U.S./International Atomic Energy Agency Safeguards Agreement, a batch is defined as "a portion of nuclear material handled as a unit for accounting purposes at a key measurement point and for which the composition and quantity are defined by a single set of specifications or measurements. Inventories are reported at the batch level of detail and the nuclear material may be in bulk form or contained in a number of separate items." Material in any one batch may have only one value for each of the following elements:

1. batch identification;
2. number of items;
3. inventory composition code;
4. key measurement point; and
5. measurement identification (i.e., measurement basis, other measurement point, and measurement method).

BEGINNING INVENTORY. The quantity of nuclear materials on hand at the beginning of an accounting period. (See also ENDING INVENTORY.)

BENT SPEAR. A formal term used by the Department of Defense for a significant incident involving a nuclear weapon/warhead or component part.

BIAS. The difference between the measured or expected value of a random variable and the corresponding true or assigned value.

BIOLOGICAL WEAPONS CONVENTION (BWC). An international treaty entered into force on March 26, 1975, that prohibits the development, production, stockpiling, acquisition, or retention of biological agents or toxins of types and in quantities having no justification for prophylactic, protective, or other peaceful purposes and weapons, equipment, or means of

delivery designed to use such agents or toxins for hostile purposes or in armed conflict, but permits defensive biological research.

BIOMETRIC DEVICE. A device that can verify an individual's identity from a physiological and/or behavioral measurement.

BLANK FIRE ADAPTER. A mechanical device attached to a firearm for the purpose of adapting it for use with blank ammunition.

BLASTING AGENTS. Any material or mixture of materials, consisting of fuel and oxidizer, intended for blasting purposes, not otherwise defined as an explosive (e.g., ammonium nitrate and fuel oil composition), provided that the resulting materials cannot be detonated by a number 8 test blasting cap when unconfined.

BOOK INVENTORY. The quantity of nuclear material present at a given time as reflected by accounting records.

BREAK-WIRE DETECTOR. An intrusion detection system sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights. An alarm is activated when the wire is broken.

BROKEN ARROW. A formal term used by the Department of Defense for an accident involving a nuclear weapon/warhead or component part.

BUILDING SECURITY HOURS. The hours designated by the cognizant security authority outside of normal working hours when additional security measures are in place.

BULK MATERIAL. Material in any physical form that is not identifiable as a discrete item, and thus must be accounted for by weight, volume, sampling, chemical analysis, or nondestructive analysis.

BULLET CONTAINMENT DEVICE. (See CLEARING BARREL.)

BULLET TRAP. A device designed to trap or capture an entire bullet and fragments as opposed to redirecting the projectile into a water or sand pit.

BYPRODUCT MATERIALS.

1. Any radioactive material (except special nuclear material) yielded in or made radioactive by exposure to the radiation incident to the process of producing or using special nuclear material; or
2. The tailings or wastes produced by the extraction or concentration of uranium or thorium from any ore processed primarily for its source material content. (42 U.S.C. 2014(e) [Section 11(e) of the Atomic Energy Act of 1954]

C

"C" MATERIALS. Special nuclear material in Attractiveness Level C. These are high grade chemical compounds, mixtures, or alloys of special nuclear material that can be converted to pure metal using relatively little processing time or effort.

CARVE-OUT. A classified contract issued in conjunction with an approved special access program (SAP) where the designated SAP security office retains inspection responsibility, in whole or in part. While the term "carve-out" technically applies only to the security functions, it also may be used to designate contract administration services, audit, review, and other functions that are performed by groups other than those who normally accomplish these tasks.

CATEGORIES OF SPECIAL NUCLEAR MATERIAL (CATEGORIES I, II, III, AND IV). A designation of the significance of nuclear material that is based on the material types, the material forms, and the amount of material.

CENTER OF MASS. The designated middle point of a specific target, usually the center point of a torso.

CENTRAL ALARM STATION. A centralized location from which a facility's intrusion detection system(s) and other security activities are monitored.

CENTRAL PERSONNEL CLEARANCE INDEX (CPCI). The Headquarters-resident automated information system established to record and be the official record of DOE access authorization transactions.

CENTRAL VERIFICATION AGENCY. A Department of Defense function responsible for verifying the facility clearance level or safeguarding capability of a contractor facility.

CERTIFICATION.

1. Comprehensive evaluation of the technical and nontechnical security features of a classified automated information system and other security measures that is made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of security requirements specified in the Classified Automated Information System Security Plan.
2. The verification that a standard of knowledge or skill level pertaining to a S&S or classification discipline has been demonstrated by testing.

CERTIFIED REFERENCE MATERIAL. Reference material, accompanied by a certificate, one or more of whose property values are certified by a procedure which establishes traceability to an accurate realization of the unit in which the property values are expressed, and for which each certified value is accompanied by an uncertainty at a stated level of confidence. (Nuclear Material Control & Accountability)

CHALLENGE INSPECTION. Under some arms control agreements, a non-routine inspection that is done on short notice of any facility under the control of a state party when requested by another state party as a right or for a noncompliance concern. Under some agreements, a right of refusal exists.

CHAMBER PORTING PROCEDURE (CPP). A machining process applied to the chambers of specific engagement simulation system (ESS) firearms that will ensure the harmless venting of cartridge gas pressure in the event of the inadvertent loading/firing of a live round and, thus, will prevent the bullet from escaping the barrel.

CHEMICAL WEAPONS CONVENTION (CWC). An international treaty entered into force on April 29, 1997, which prohibits the development, production, acquisition, stockpiling, transfer, and use of chemical weapons, and monitors non-prohibited chemical activity.

CLASSIFICATION. The act or process by which information or matter is determined to require protection in the interest of national security under either 42 U.S.C. 2162 (Section 142, as amended, of the Atomic Energy Act) or Executive Order 12958, as amended.

CLASSIFICATION AUTHORITY. The authority that is vested in an individual to determine that information or matter requires protection against unauthorized disclosure in the interest of national security. (See also ORIGINAL CLASSIFIER and DERIVATIVE CLASSIFIER.)

CLASSIFICATION CATEGORY. One of the three kinds of classified information: Restricted Data, Formerly Restricted Data, or National Security Information.

CLASSIFICATION GUIDANCE. A written record of detailed instructions as to whether specific information is classified, usually concerning a system, plan, project, or program. The guidance identifies information to be classified and specifies the level (and duration for National Security Information only) and category of classification assigned to such information.

CLASSIFICATION LEVEL. A designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized people. The three classification levels in descending order of potential damage are Top Secret, Secret, and Confidential.

CLASSIFICATION MARKINGS. A designation on classified matter consisting of the following elements: classification level, classification category (if Restricted Data or Formerly Restricted Data), caveats (special markings), classifier information, and originator identification.

CLASSIFICATION OFFICER.

1. Field Element Classification Officer: An individual designated to administer the classification program for that particular field element and to monitor the classified programs of contactors under its cognizance.

2. Contractor Classification Officer: An individual designated to administer the classification program for that particular contractor and to monitor the classified programs of subcontactors under its cognizance.

CLASSIFIED AUTOMATED INFORMATION SYSTEM. An automated information system itself and its additional features and assurances, if any, that enhance its secure operation that is accredited for processing classified information.

CLASSIFIED COMPUTER SECURITY PROGRAM. All of the technological protection measures and administrative requirements established and applied to classified automated information systems (including computer hardware, software, and data) and their facilities to ensure the protection of classified information.

CLASSIFIED CONFIGURATION. An item that by virtue of its visual characteristics reveals classified information.

CLASSIFIED INFORMATION. Information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, or information determined to require protection against unauthorized disclosure under Executive Order 12958, *Classified National Security Information*, as amended, or prior executive orders, which is identified as National Security Information.

CLASSIFIED MAILING ADDRESS (CMA). An authorized mail address, including ZIP Code, for which procedures for classified mail deliveries have been approved.

CLASSIFIED MATERIAL. Chemical compounds, metals, fabricated or processed items, machinery, electronic equipment, and other equipment or any combination thereof containing or revealing classified information.

CLASSIFIED MATTER. Any combination of documents and material containing classified information. This includes explosives whose shape is classified and classified parts.

CLASSIFIED REMOVABLE ELECTRONIC MEDIA (CREM). Any item or material (medium) that (1) can retain digital information; (2) is required to be marked as classified; (3) requires electric power to function as intended; and (4) is designed, intended, or permitted to be removed or transported by a user of the medium.

CLASSIFIED SHIPPING ADDRESS. An authorized location for the delivery of classified matter that cannot be transmitted by mail and for which procedures for classified freight receipt have been approved.

CLASSIFIED VISIT. A visit that will involve or is expected to involve access to, or an exchange of, classified information.

CLASSIFIER. An individual who makes a classification determination. (See also ORIGINAL CLASSIFIER or DERIVATIVE CLASSIFIER.)

CLEAR. To ensure that a firearm has no cartridge in the chamber, cylinder, or loading mechanism and, if magazine-fed, that the magazine is removed.

CLEARING BARREL. A device that a weapon is pointed at or into during the loading and unloading process that will contain inadvertently discharged rounds.

CLEAR ZONE. An area within the site perimeter and around the boundary of the site free of all obstacles, topographical features, and vegetation exceeding a specified height. The zone is designed to facilitate detection and observation of an intruder, to deny protection and concealment to an intruder, to maximize effectiveness of the protective force, and to reduce the possibility of a surprise attack.

CLOSURE. The process of completing transaction system entries for an accounting period; adjusting the accounts to reflect radioactive decay, improved accountability measurements, estimates and measurements of holdups, and operational losses; reconciling with the physical inventory (if any); correcting data entry and other errors in the accounting system; posting gains or losses to the material balance area inventory accounts; and reconciling to the national nuclear materials accounts (i.e., the Nuclear Materials Management and Safeguards System). The accounts are closed periodically to establish and document the nuclear materials inventory at a specific point in time. (Nuclear Material Control & Accountability)

CODE WORD. A word, approved by DOE or another Federal agency, for which at least one definition is (or was) classified. Code words must not suggest the nature of their meaning or convey the nature of the protected activity. Code words pertaining to special access programs are usually classified.

COGNIZANT SECURITY AUTHORITY. DOE and NNSA Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

COMMUNICATIONS SECURITY (COMSEC). Measures and controls taken to deny unauthorized people information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: COMSEC includes cryptosecurity, transmission security, emission security, and physical protection of COMSEC material.

COMPENSATORY MEASURE. Temporary safeguards or security activity designed to afford equivalent protection for safeguards or security interests when a protection system element has failed or new requirement or vulnerability has been identified.

COMPOSITE ADVERSARY TEAM. Designated individuals from selected sites who act the part of adversaries during performance tests.

COMPOSITE FACILITY RATING. An overall rating that reflects a balance of S&S program performance and compliance topical rating results as determined by the surveying organization.

COMPOSITION. The qualitative and quantitative makeup of a chemical compound. The composition of a nuclear material may be described in terms of the relative concentrations of its constituents.

COMPOSITION OF ENDING INVENTORY CODES. Predefined codes assigned to inventory descriptions arranged in logical groupings according to usage, process, and chemical and physical form. Descriptors are included to identify group headers and group totals.

COMPREHENSIVE BRIEFING. A briefing required before one is granted access to classified matter and/or special nuclear material, designed to inform individuals who are granted a DOE access authorization (security clearance) of their responsibilities.

COMPROMISE. Disclosure of classified or unclassified controlled information to unauthorized person(s). (See also UNAUTHORIZED DISCLOSURE.)

COMPROMISING EMANATIONS. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

COMPUTER SECURITY. The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

CONCENTRIC SECURITY AREAS. A series of physical spaces designated as security areas surrounding a designated S&S interest. These security areas; i.e., property protection, limited, exclusion, protected, vital, and material access areas, provide for the imposition of graded physical protection measures which entail controlling access to and egress from the designated areas and security interests. Security areas are delineated by separate and distinct barriers and/or controls.

CONCISE NOTE. Additional nuclear materials transaction, material balance, or inventory data supplied to the International Atomic Energy Agency, in free text format, by facilities selected under the *Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States*, and by facilities engaged in the import and/or export of nuclear materials.

CONFIDENTIAL. A classification level that is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

CONFIRMATION MEASUREMENT. A qualitative or quantitative measurement made to verify the integrity of an item by testing whether some attribute or characteristic of the nuclear material in the item is consistent with the expected attribute or characteristic of the material. The measurement method used for confirmatory measurements must be capable of determining the presence of a specific attribute of the material, consistent with valid acceptance and rejection criteria.

CONTAINMENT. The effect achieved by S&S systems and personnel that prevents an adversary or special nuclear material from leaving a particular space, structure, or facility. (See also MATERIAL CONTAINMENT.)

CONTINUOUS VISUAL SURVEILLANCE. Unobstructed view at all times of special nuclear material or other S&S interest, and/or of all access to a storage area or cargo compartment containing the material or interest.

CONTROL.

1. The authority of the agency that originates information, or its successor in function, to regulate access to the information. (Executive Order 12958, *Classified National Security Information*, as amended).
2. The application of systems, devices, or procedures that allows timely authorized use while precluding or delaying unauthorized use.

CONTROLLED ARTICLES. Articles controlled because of their potential to be used to record or transmit information without authorization. Examples include recording equipment (audio, video, optical, or data); electronic equipment with a data exchange port capable of being connected to automated information system equipment; cellular telephones; radio frequency transmitting equipment; and computers and associated media.

CONTROLLED CRYPTOGRAPHIC ITEM. Secure telecommunications or information handling equipment, or associated cryptographic component or ancillary device which is unclassified when unkeyed (or when keyed with an unclassified key) but controlled. Equipment and components so designated bear the designator "Controlled Cryptographic Item."

CONTROLLED INTERFACE. The software, hardware, firmware, and equipment that mediate the differences in security and need-to-know between attached automated information systems.

CONTROL LIMIT. The established value beyond which any variation, such as inventory difference, is considered to indicate the possibility of an assignable cause. Control limits include warning limits or alarm limits. (See also ALARM LIMIT and WARNING LIMIT.) (Nuclear Material Control & Accountability)

CONVENTION FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIALS (CPPNM). An international treaty that entered into force in 1987 which requires specific levels of protection for nuclear materials in international transport.

COSMIC. A North Atlantic Treaty Organization (NATO) marking applied to all copies of Top Secret documents prepared for circulation within NATO.

COUNTERINTELLIGENCE. The information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, information, or communications security programs.

COUNTERMEASURES.

1. Activities or capabilities that are designed to negate an adversary's ability to exploit vulnerabilities.
2. Under treaties, use of devices and/or techniques to protect national security, proprietary information, or other critical information while fulfilling state party treaty obligations.

COUNTRY CONTROL NUMBER. An eight-character coded identifier used in nuclear materials documentation and reporting to indicate the country of origin of nuclear materials; the country providing isotopic separation services that originally produced the depleted or enriched uranium; the country in which reactor products were produced; and the country or international organization with any special safeguards conditions attached to the materials' use or transfer. (Nuclear Material Control & Accountability)

COVER SHEET. A paper developed to protect classified and unclassified controlled information from inadvertent disclosure and to alert observers to the classification level and category or type of unclassified controlled information in the attached matter.

CREDENTIAL. A document which identifies the intended bearer and indicates that he/she has the authority to perform specific functions (e.g., authority to carry firearms, authority to arrest).

CREDIBLE ROLL-UP. Roll-up is determined to be credible based on a vulnerability analysis consistent with the Design Basis Threat. (See ROLL-UP.)

CREDIBLE SUBSTITUTION MATERIAL. Material that can be successfully used in place of accountable special nuclear material. This substitution is possible because of one or more physical properties shared by the substitution material and the special nuclear material.

CRITICAL FACILITY. A facility designated by either the Secretary or a Departmental Element that requires Threat Level 3 protection due to its high value or criticality to national security or Departmental needs.

CRITICAL INFORMATION. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries or competitors for them to plan and act effectively to guarantee failure or unacceptable consequences for mission accomplishment.

CRITICAL PATH SCENARIO. An adversary-based scenario that is generated during the conduct of a vulnerability assessment and accounts for adversary tactics that minimize the probability of interruption (P_I) and/or neutralization (P_N) for a given protection system. More than one scenario may be generated, one of which will produce the lowest system effectiveness (P_E) values/ratings.

CRITICAL PROGRAM INFORMATION. Information concerning sensitive activities, whether classified or unclassified, that is vitally needed by adversaries or competitors for them to plan and act effectively. NOTE: Formerly, that information on what was called the "critical and sensitive information list." (Operations Security)

CRITICAL SYSTEM ELEMENT. A component or subcomponent of an S&S protection system that directly affects the ability of the system to perform a required function. Critical components may be equipment, procedures, or personnel.

CRYPTO. The marking or designator identifying Communications Security keying material used to secure or authenticate telecommunications carrying classified or sensitive Government or Government-derived information. NOTE: When written in all upper case letters, CRYPTO has the meaning stated above. When written in lower case as a prefix, crypto and crypt are abbreviations for cryptographic.

CRYPTOSYSTEM. Associated Information Security items interacting to provide a single means of encryption or decryption.

CUSTODIAN. Any person who has possession of classified matter or other S&S interest, or is charged with, or otherwise has assigned responsibility for, the control and accountability of such an interest. (See also NUCLEAR MATERIALS CUSTODIAN.)

CYBER SECURITY. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

D

"D" MATERIALS. Special nuclear material in Attractiveness Level D. This is bulk and low-purity special nuclear material that requires extensive processing time or complex processing to convert the material to a high grade or metal form.

DAILY ADMINISTRATIVE CHECK. A daily review to provide timely identification of obvious abnormalities or missing items, or to ascertain that there is no indication of tampering.

DAMAGE ASSESSMENT. An analysis of the impact on national security of an actual compromise or unauthorized disclosure of classified information.

DEADLY FORCE. The force that a reasonable person would consider likely to cause death or serious bodily harm.

DECISION SHOOTING. Practical application of an individual's decision-making ability in the use of deadly force.

DECLASSIFICATION. A determination by an appropriate authority that information or matter no longer requires protection as classified information against unauthorized disclosure because of national security concerns.

DECRYPT. To convert encrypted text into its equivalent plain text by means of a cryptosystem. (This does not include solution by cryptanalysis.) NOTE: The term "decrypt" includes both deciphering and decoding.

DEFENSE-IN-DEPTH. The use of multiple, independent protection elements combined in a layered manner so that system capabilities do not depend on a single component to maintain effective protection against defined threats.

DELAY. The effect achieved by physical features, technical devices, security measures, or protective forces that impedes an adversary from gaining access to an asset being protected or from completing a malevolent act.

DELAY MECHANISM. A mechanism employed to impede removal or unauthorized use of Departmental property, such as passive barriers (e.g., walls, ceilings, floors, windows, doors, security bars), activated barriers (e.g., sticky foam, pop-up barriers), and visual obscurants (e.g., cold smoke).

DENIAL. The effect achieved by S&S systems or devices that prevents a potential intruder or adversary from gaining access to or use of a particular space, structure, facility, or asset.

DENIAL OF ACCESS. The engagement and neutralization of the adversary prior to the adversary acquiring hands-on access to the material or asset.

DENIAL OF TASK. The prevention and/or neutralization of a threat to preclude the completion of a specified task. This could include (1) interrupting an adversary in the conduct of a specified task prior to the completion of task time, (2) physical barriers that prohibit the completion of a given task (e.g., increased standoff distance for vehicle bombs, segregation of material to preclude an unacceptable material dispersion), (3) protection measures that prevent the introduction of the materials or items required to cause the postulated event, or (4) denying necessary information about or access to an asset.

DEPARTMENTAL PROPERTY. All land, buildings, and structures (real property) and other property which are owned, rented, or leased by the United States and subject to the administrative custody or jurisdiction of the Department.

DEPLETED URANIUM. Uranium containing less uranium-235 than the naturally occurring distribution of uranium isotopes (less than 0.711 percent by weight).

DERIVATIVE CLASSIFICATION. A determination based on classification guidance or source documents that matter contains Restricted Data, Formerly Restricted Data, and/or National Security Information.

DERIVATIVE CLASSIFIER. An individual authorized to determine that matter is unclassified or classified as Restricted Data, Formerly Restricted Data, and/or National Security Information and at what level based on classification guidance or source documents.

DERIVATIVE DECLASSIFIER. An individual authorized to declassify or downgrade matter in specified areas based on classification or declassification guidance or source documents.

DEROGATORY INFORMATION. Any factual and verifiable unfavorable information that creates a question as to an individual's eligibility for an access authorization. (10 CFR 710.8, *Criteria*)

DESIGNATED APPROVING AUTHORITY. The official with the authority to formally grant approval for operating a classified automated information system; the person who determines the acceptability of the residual risk in a system that is prepared to process classified information and either accredits or denies operation of the system.

DESIGNATED DISCLOSURE AUTHORITY. An official designated by the head of an agency or by the agency's principal disclosure authority to control disclosures of classified information.

DESIGN BASIS THREAT (DBT). The statement that describes threats that are postulated for the purpose of analyzing S&S programs, systems, components, equipment, information, or material [see DOE O 470.3, *Design Basis Threat Policy (U)*].

DESTRUCTION. The physical alteration of classified matter which precludes the reconstruction and recovery of classified information.

DETECTION.

1. The positive assessment that a specific object is the cause of the alarm.
2. The announcement of a potential malevolent act through alarms.

DETECTION LIMIT. The threshold quantity at which a detector indicates the presence of a phenomenon. (Modified from International Standards Organization 1993.) (Nuclear Material Control & Accountability)

DETECTION ZONE. A volume of space or surface area under the surveillance of one or more intrusion detection devices from which an alarm is produced when the volume or surface area is subject to a condition for an alarm.

DETONATING CORD. A flexible cord containing a center core of high explosives used to detonate other explosives.

DEVIATION. A condition that diverges from the norm and that is categorized as a variance, waiver, or exception according to the degree of risk accepted.

DIRECT ACCESS. Access to Category I quantities of special nuclear material which would permit an individual to remove, divert, or misuse that material in spite of any controls that have been established to prevent such unauthorized actions. (Category I quantities of special nuclear material are defined in DOE M 470.4-6, *Nuclear Material Control and Accountability*.)

DIRECT-USE (MATERIAL). Nuclear material that can be used for the manufacture of nuclear explosives components without transmutation or further enrichment.

DIVERSION.

1. The unauthorized removal of nuclear material from its approved use or authorized location.
2. An act that attempts to reposition the protective force to a location other than where the actual adversarial action is taking place. (See also LOSS and THEFT.)

DOCUMENT. A physical medium, regardless of its physical form or characteristic, used to convey information.

DOE COGNIZANT SECURITY AUTHORITY. DOE and NNSA Federal employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

DOE LINE MANAGEMENT. DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

DOWNGRADE. A determination by an appropriate authority that (1) information may be handled at a level lower than the initial classification level or (2) matter may be handled at a level and/or category lower than the initial classification level and/or category, but in either case, not lower than Confidential.

DRY FIRE. To manipulate a firearm and practice firing with no live cartridges or to use dummy ammunition.

DULL SWORD. A formal term used by the Department of Defense to identify and report a nuclear weapons safety deficiency.

DURESS SYSTEM. A system with notification capabilities that when activated indicates an individual is experiencing a threatening situation or coercion.

E

"E" MATERIALS. Special nuclear material in Attractiveness Level E. These are not covered by Attractiveness Levels A through D and include highly radioactive special nuclear material, solutions containing less than 1 gram special nuclear material per liter of solution, and uranium enriched to less than 20 percent uranium-235.

EARLY WARNING SYSTEM. An intrusion detection system that can detect intrusions beyond a protected perimeter.

EFFECTIVENESS TEST. A test to confirm that an essential element or total system is operating as required and can effectively perform a specified function.

EMISSION SECURITY. The protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system.

EMPTY QUIVER. A formal term used by the Department of Defense in reporting the seizure, theft, or loss of a U.S. nuclear weapon.

ENDING INVENTORY. The quantity of nuclear materials on hand at the end of an accounting period. Inventory as of the close of business of the last day of the report period. (See also BEGINNING INVENTORY.)

ENRICHED URANIUM. Uranium which contains more of the fissionable isotope uranium-235 than the naturally occurring fraction, which is defined as 0.00711 by weight, or 0.711 percent.

ENTRY CONTROL POINT. An entrance to a secured area at which ingress and egress are controlled.

ENTRY INTO FORCE. The initial date the provisions of a treaty become effective.

ESCORT.

1. An authorized individual having the responsibility to oversee and control people in a security area who do not have the proper need-to-know or access authorizations for the security area.
2. An authorized individual or common carrier employee with the responsibility to accompany personnel or matter while in transit.

ESSENTIAL ELEMENT. The equipment, procedures, or personnel components of a S&S system whose failure would reduce protection of Departmental property to an unacceptable level.

ESTIMATE. A technically defensible approximation of the quantity of nuclear material based on process parameters and/or material attributes. An estimate is used when a direct measurement of the nuclear material amount is not possible. (Nuclear Material Control & Accountability)

EURATOM. An organization (legal entity) comprised of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

EXCEPTION. An approved deviation from a DOE directive for which DOE accepts the risk of an S&S vulnerability.

EXCLUSION AREA (EA). A type of security area defined by physical barriers and subject to access control where mere presence in the area would normally result in access to classified information.

EXECUTIVE PROTECTION OPERATION. All the security activities, from information gathering to actual physical protection, to provide armed executive protection to the principal. The operation covers a specific period of time and a specific location (or locations).

EXERCISE. An enactment of a scenario that simulates an actual incident requiring a response.

EXPLAINED INVENTORY DIFFERENCE. The portion of the inventory difference accounted for and reported to the Nuclear Materials Management and Safeguards System in one of the following categories: re-determination of discrete items on inventory, re-determination of material in process, process holdup differences, equipment holdup differences, measurement adjustments, rounding, recording and reporting errors, shipper-receiver adjustments, or identifiable item adjustments.

EXPORT CONTROLLED INFORMATION. Certain unclassified Government information under the Department's cognizance that, if generated by the private sector, would require a specific license or authorization for export under regulations. Information and technology regulated by the Export Administration Regulations, 15 CFR Parts 742, 744, and 746, and the International Traffic in Arms Regulations, 22 CFR 120.21.

EXTERNAL TRANSFER. The transfer of nuclear materials from one reporting identification symbol (RIS) to another. (Nuclear Material Control & Accountability)

F

FACILITY. An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected by the Department, the U.S. Nuclear Regulatory Commission, or their contractors.

FACILITY CLEARANCE. An administrative determination that a facility is eligible to access, receive, produce, use, and/or store classified matter, nuclear materials, or Departmental property of significant monetary value.

FACILITY CODE. The unique numeric value assigned to a facility when it has been granted a facility clearance.

FACILITY DATA AND APPROVAL RECORD (FDAR). A DOE form (DOE F 470.2) used to record approvals and deletions of and changes to facility information.

FACILITY IMPORTANCE RATING. A ranking which identifies the Departmental interest or property and its associated survey frequency. (See DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.)

FACILITY SECURITY OFFICER (FSO). A U.S. citizen, with an access authorization equivalent to the facility clearance, assigned the responsibility of administering the requirements of the S&S Program within the facility.

FADED GIANT. A formal term used by the Department of Defense to identify an event involving a nuclear reactor or radiological accident.

FALSE ALARM. An alarm, generated internal to the sensor equipment, for which the specific cause is unknown.

FERTILE MATERIAL. Material composed of atoms which readily absorb neutrons to produce fissile material (e.g., uranium-238 or thorium-232, which produce plutonium-239 and uranium-233, respectively). Fertile material alone cannot sustain a chain reaction.

FIELD PROCESSOR. An intelligent processor responsible for direct monitor and control of sensors, alarm groups, actuators, portals, and user entry devices.

FINDING. A factual statement of validated deficiencies resulting from an inspection and/or assessment activity.

FINGERPRINT.

1. An ink or other impression of the curves formed by the ridges on fingertip skin used as a way of identifying persons.
2. The unique characteristics of an item or material, such as relative gamma count at specified energies with total passive neutron count rate. (Nuclear Material Control & Accountability)

FISSILE ISOTOPE. Uranium-233, uranium-235 by enrichment category, plutonium-239, and plutonium-241.

FISSILE MATERIAL.

1. A material capable of undergoing fission by interaction with slow neutrons. (More restrictive than *fissionable*.) (*IAEA Safety Glossary*)
2. A material that releases energy by the fission process when it absorbs thermal or slow-moving neutrons; the principal fissile materials are uranium-233, uranium-235, and plutonium-239. (*Academic Press Dictionary of Science and Technology*)

FISSILE MATERIAL CONTAMINATION. The release of fissile material in excess of that controlled and monitored by Departmental radiological protection programs.

FISSILE MATERIAL DISPERSAL. The aerosolization and transport of fissile material by a driving force, such as fire, high-explosive deflagration, or high-explosive detonation.

FISSION PRODUCTS.

1. The radionuclides produced by nuclear fission. Used in contexts where the radiation emitted by the radionuclides is the potential hazard. (*IAEA Safety Glossary*)
2. A general term for the complex mixture of substances produced as a result of nuclear fission.

FORCE-ON-FORCE (FOF) EXERCISE. An exercise that uses protective force or other designated personnel in the role of an adversary force to simulate the actual engagement of protective forces.

FORCE OPTIONS. The tactical means that are available to a special response team including, but not limited to, open air assault, mobile assault, emergency assault, and stronghold assault using dynamic and covert entry techniques to effect interdiction, interruption, neutralization, and recovery operations (e.g., resolution of a terrorist situation, or the protection of special nuclear material from theft or sabotage).

FORECASTS. The projections of nuclear material inventories, requirements, returns, and transactions for existing and planned user projects.

FOREIGN GOVERNMENT INFORMATION (FGI). Information that is:

1. provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
2. produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any elements thereof, requiring that the information, the arrangement, or both are to be held in confidence; or
3. received and treated as "Foreign Government Information" under the terms of a predecessor order. (Executive Order 12958, *Classified National Security Information*, as amended)

FOREIGN NATIONAL. Any person who is not a U.S. citizen (i.e., not a U.S. national); any corporation not incorporated in the U.S.; any international organization; foreign government; or any agency or subdivision of foreign government (e.g., diplomatic missions). (Security)

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI). The condition that exists when a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of a U.S. company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may adversely affect the performance of classified contracts.

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE DETERMINATION. A determination rendered by the Government as to whether a U.S. company requiring facility clearance in order to perform work requiring access to classified information and/or special nuclear material or the granting of access authorizations is or may be subject to foreign ownership, control, or influence.

FORM. The shape or internal structure of a material. Nuclear materials may be metals or be constituents of an alloy, an oxide or other solid compound, a solution, or a gas. (Nuclear Material Control & Accountability)

FORMERLY RESTRICTED DATA (FRD). Classified information jointly determined by the DOE or its predecessor agencies and the Department of Defense to be (1) related primarily to the military utilization of atomic weapons and (2) protected as National Security Information. It is subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

FOR OFFICIAL USE ONLY (FOUO). A control marking used by the Department of Defense and some other agencies to identify information that may be withheld from public disclosure under the criteria of the Freedom of Information Act.

FRESH PURSUIT. The pursuit (with or without a warrant) of any person who commits a misdemeanor or felony or is suspected of having committed a misdemeanor or felony for the purpose of preventing escape or effecting an arrest. The pursuit must be without unreasonable delay, but need not be immediate pursuit.

FUNCTIONAL TEST. A test of a sensor that determines whether the minimum design requirements for the sensor are being met (e.g., for an interior microwave intrusion detection sensor, a functional test would confirm that the detection pattern and orientation are within design limits).

G

GAIN (PHYSICAL INVENTORY). An inventory difference showing an ending physical inventory larger than the book inventory. (Nuclear Material Control & Accountability)

GOVERNMENT-OWNED EQUIPMENT/PROPERTY. All land, buildings, and structures (real property) and portable equipment, records, and supplies (other property) that are owned, rented, or leased by the Government and subject to the administrative custody or jurisdiction of DOE.

GRADED PROTECTION. The policies and S&S measures (level of effort and resources) that are applied in a proportional manner toward the protection of S&S interests based on the impact of their loss, destruction, or misuse.

GRADED SAFEGUARDS.

1. A system designed to provide varying degrees of physical protection, accountability, and material control to different types, quantities, physical forms, and chemical or isotopic compositions of nuclear materials consistent with the risks and consequences associated with threat scenarios.
2. A system designed to provide the greatest relative amount of control and effort to the types and quantities of special nuclear material that can be most effectively used in a nuclear explosive device.

H

HARDENED STRUCTURES. Exterior walls, windows, doors, and floors and/or roof constructed of, or reinforced with, materials that have bullet-penetration resistance equivalent to the "high-powered rifle" rating in Underwriters Laboratories Inc. Standard 752, *Standard for Safety for Bullet-Resisting Equipment*.

HIGH ENRICHED URANIUM (HEU). Uranium enriched to 20 percent or greater in the isotope uranium-235.

HIGH EXPLOSIVES. Explosive substances capable of mass detonation, and for which there is a significant probability of accidental initiation or transition from burning to detonation.

HIGH-LEVEL RADIOACTIVE WASTE (HLW). (NOTE: Also called HIGH-LEVEL WASTE) The highly radioactive material resulting from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations, and other highly radioactive material that the U.S. Nuclear Regulatory Commission, consistent with existing law, determines by rule requires permanent isolation. (42 U.S.C. 10101, *Nuclear Waste Policy Act of 1982*, and 10 CFR 72, *Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-level Radioactive Waste*)

HIGH-LEVEL WASTE. See HIGH-LEVEL RADIOACTIVE WASTE.

HIGHLY IRRADIATED MATERIAL. Material having a radiation level of at least 100 rem per hour at 1 meter.

HOLDUP. The amount of nuclear material remaining in process equipment and facilities after the in-process material, stored materials, and product have been removed and the facility has been cleaned as well as possible. NOTE: Holdup material is reflected as part of a facility's inventory record with justified estimates or measured values of material.

HUMAN RELIABILITY PROGRAM (HRP). A security and safety reliability program designed to ensure that individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities, and programs meet the highest standards of reliability and physical and mental stability.

I

ILLEGAL DRUGS. A controlled substance, which is identified in 21 U.S.C. 802(6) as a drug included in Schedule I, II, III, IV, or V, as set by 21 U.S.C. 812 and made unlawful under 21 U.S.C. Chapter 13, Part D. The term "illegal drugs" does not apply to the use of a controlled substance in accordance with the terms of a valid prescription, or other uses authorized by law.

IMPACT AREA. That area in a backstop or bullet trap directly behind the target where bullets are expected to impact. The term also may refer to a safety zone or area down range of an outdoor range where bullets will impact if not captured in a backstop.

IMPROVISED EXPLOSIVE DEVICE. A non-commercial/non-military device consisting of an explosive/incendiary and firing components necessary to initiate the device. Similar in nature to a grenade, mine, or bomb.

IMPROVISED NUCLEAR DEVICE (IND). A device made outside an official Government or other nuclear-weapon-state program and which has, appears to have, or is claimed to have the capability to produce a nuclear detonation.

INCENDIARY DEVICE. Any self-contained device intended to create an intense fire that can damage normally flame-resistant or retardant materials.

INCIDENT REPORT. A report of any event of security concern to the DOE, DOE interest, or national security.

INCIDENTS OF SECURITY CONCERN. Events which are of concern to the DOE S&S Program that warrant preliminary inquiry and subsequent reporting.

INDICATORS. Sources of information that, if exploited by an adversary or competitor, could reveal critical program information. An indicator can be identified by asking the question, "If I were an adversary or competitor, where would I go to obtain critical program information?" NOTE: Formerly called "essential elements of friendly information." (Operations Security)

INDICES CHECKS. A procedure whereby an inquiry is made to the investigative and intelligence files of appropriate Federal agencies to determine whether there is information of record on a particular individual.

INDUSTRIAL ESPIONAGE. The gathering of proprietary data from private companies or the Government by non-Government representatives for the purpose of helping other companies to improve their competitive advantage.

INDUSTRIAL SECURITY. A multi-disciplinary security program concerned with the protection of classified information and other Departmental property developed by or entrusted to U.S. industry.

INFORMATION. Facts, data, or knowledge itself as opposed to the medium in which it is contained.

INFORMATION SECURITY. A system of administrative policies and procedures for identifying, marking, and protecting from unauthorized disclosure, information that is authorized protection by executive order or statute.

INFRACTION.

1. Any knowing, willful, or negligent action contrary to the requirements of Executive Order 12958, *Classified National Security Information*, as amended, or its implementing directives that does not constitute a "violation."
2. The documentation of administrative and/or disciplinary actions assigned to an individual taken in response to an incident of security concern.

INITIAL BRIEFING. A briefing to inform individuals of security procedures and access control requirements, conducted before said individuals assume their duties at a Departmental facility.

IN-PROCESS INVENTORY. The quantity of nuclear material in a process area at any specified time, excluding holdup. (Nuclear Material Control & Accountability)

INQUIRY. A review of the circumstances surrounding an incident of security concern to develop all pertinent information and to determine whether an infraction, violation, or a compromise or potential compromise has occurred.

INSIDER. A person who, by reason of official duties, has knowledge of operations and/or security system characteristics, and/or position that would significantly enhance the likelihood of successful bypass or defeat of positive measures should that person attempt such an action.

INSPECTION. The process of gathering information to determine the effectiveness with which protection programs are implemented.

INSPECTION EQUIPMENT. Specific treaty-authorized verification equipment used for an onsite inspection under a treaty or international agreement.

INSPECTION MANDATE. Under a variety of treaties, the authority and instructions issued by the Technical Secretariat of the inspection organization to the inspection team for the conduct of a particular inspection.

INTERDICT. To stop or delay an adversary before he/she reaches or achieves his/her objective.

INTERIM ACCESS AUTHORIZATION. A determination to grant an access authorization before receipt and adjudication of an individual's completed background investigation.

INTERNAL CONTROL SYSTEM. A system of administrative and accounting policies and procedures implemented by a facility to ensure proper functioning of the material control and accountability system. (Nuclear Material Control & Accountability)

INTERNAL REVIEW. An examination of practices and procedures by the responsible organization in sufficient detail to determine if a system is appropriate and is performing as intended.

INTERNAL TRANSFER. The transfer of nuclear material within the same reporting identification symbol (RIS). (Nuclear Material Control & Accountability)

INTERNATIONAL (MEASUREMENT) STANDARD. A standard recognized by an international agreement to serve internationally as the basis for assigning values to other standards of the quantity and material composition concerned.

INTERNATIONAL NUCLEAR MATERIALS TRACKING SYSTEM. A database and information support system used to manage information on the quantity and location of U.S.-supplied nuclear materials in foreign countries.

INTERNATIONAL SAFEGUARDS. Under the Treaty on the Non-Proliferation of Nuclear Weapons (Nuclear Non-Proliferation Treaty), the verification measures imposed by the International Atomic Energy Agency to prevent the diversion of nuclear material from peaceful uses to nuclear weapons or other nuclear explosive devices.

INTERRUPT. To disrupt an adversarial activity before it reaches or achieves its objective.

INTRINSICALLY TAMPER-INDICATING. An item (i.e., a single piece or container of nuclear material) that is constructed in such a manner that a malevolent act cannot be accomplished without permanently altering it in a manner that would be obvious during visual inspection.

INTRUSION DETECTION SYSTEM (IDS). A security system consisting of sensors capable of detecting one or more types of phenomena, signal media, annunciators, energy sources, alarm assessment systems, and alarm reporting elements, including alarm communications and information display equipment.

INVENTORY. (See also BOOK INVENTORY and PHYSICAL INVENTORY.)

1. A complete, detailed, descriptive record of classified document holdings with the capability of making it consistent or compatible with documents on hand (reconciliation).
2. The act of comparing documents to records of holdings.

INVENTORY DIFFERENCE.

1. The difference between the nuclear material book inventory and the corresponding physical inventory adjusted for transfers in and out of the material balance area.
2. The quantity given by the following equation:

$$ID = BI - EI + TI - TO$$

where ID is the inventory difference; BI and EI are the beginning and ending inventories, respectively; and TI and TO are the transfers of nuclear material into and out of the material balance area, respectively.

INVENTORY RECONCILIATION. The process of comparing, investigating discrepancies, and adjusting the book inventory to the corresponding physical inventory.

INVESTIGATION. (See also BACKGROUND INVESTIGATION.)

1. A review of the circumstances surrounding an incident of security concern by law enforcement entities.
2. A process used to gain an understanding of an MC&A discrepancy, incident, or alarm, its cause(s), and, if the situation is not satisfactorily resolved, the corrective action(s) necessary to prevent recurrence or remedy the problem. (Nuclear Material Control & Accountability)

IRRADIATED NUCLEAR MATERIAL. Nuclear material that, in its existing form, has been subjected to irradiation in a nuclear reactor or accelerator and that consequently delivers an external radiation dose requiring special containment and handling.

ISOLATION ZONE. Any area adjacent to a physical barrier, cleared of all objects which could conceal or shield an individual. (See also CLEAR ZONE.)

ITEM.

1. A single piece or container of nuclear material which has a unique identification and a known nuclear material mass, and whose presence can be visually verified.
2. Any discrete quantity or container of special nuclear material or source material, not undergoing processing, having a unique identity, and also having an assigned element and isotope quantity. (10 CFR 74.4, *Definitions*) (Nuclear Material Control & Accountability)

J

JOB ANALYSIS. A systematic method used to obtain a detailed listing of the tasks of a specific job.

JOB/TASK ANALYSIS (JTA). A process that describes systematically the performance requirements of a job by identifying and defining the valid tasks and the elements needed to satisfactorily perform the analyzed job.

JOINT TRAINING EXERCISE (JTE). An exercise consisting of a force-on-force exercise that includes outside agencies to determine the agencies' abilities and capabilities to respond to site threats, as documented in the site safeguards and security plan or site security plan.

K

KEY. Usually a sequence of random or pseudorandom bits used to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, determining electronic counter-countermeasure patterns, or producing other keys. (Computer Security)

KEYING MATERIAL. Key, code, or authentication information in physical or magnetic form.

KEY MANAGEMENT PERSONNEL (KMP). Owners, officers, directors, executive personnel, general partners, regents, trustees and so forth of a contractor organization identified by the Department during the foreign ownership, control, or influence (FOCI) process as requiring access authorizations.

KEY MEASUREMENT POINT. A location where nuclear material appears in such a form that it may be measured to determine material flow or inventory. Includes, but is not limited to, the inputs and outputs (including measured discards) and holdings in material balance areas. (Nuclear Material Control & Accountability)

L

L ACCESS AUTHORIZATION. A type of authorization granted by the Department indicating that the recipient is approved for access to the following levels and categories of classified information on a need-to-know basis: Confidential Restricted Data, Secret and Confidential National Security Information, and Secret and Confidential Formerly Restricted Data.

LAYOVER FACILITY/SAFE HAVEN. A Departmental, Departmental contractor, or U.S. Department of Defense facility that provides proper security for shipment vehicles, material, and equipment while personnel are in rest-overnight status.

LICENSED MATERIAL. By-product material, source material, or special nuclear material received, possessed, used, or transferred under a general or specific license issued by the U.S. Nuclear Regulatory Commission (10 CFR 30 through 40).

LIMITED AREA (LA). A type of security area having boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized people to classified matter or special nuclear material.

LIMITED FACILITY CLEARANCE. A facility clearance (FCL) with access limitations. Limited FCLs severely restrict a company's access to classified information (e.g., not valid for access to Top Secret information, Restricted Data, Formerly Restricted Data, Communications Security information, Arms Control and Disarmament Agency classified information, and information that has not been determined releasable by designated Government disclosure authorities to the country from which the company's ownership is derived).

LIMITED-LIFE COMPONENT. A nuclear weapon component that deteriorates in some respect over time and must be replaced periodically during the weapon stockpile lifetime. Principal classes of limited-life components are reservoirs, neutron generators, and parachutes.

LIMITED PROCESSING. Processing of special nuclear material which changes a few characteristics but not the overall form of the material in a particular item. Specific examples of limited processing may include homogenization, dissolution, or firing of an oxide to obtain a more stable oxide.

LIMITED-SCOPE PERFORMANCE TEST (LSPT). A performance test designed to evaluate specific skills, equipment, operations, or procedures. The events of the test may be interrupted to facilitate data collection, and they may be purposely directed by evaluators in order to achieve certain evaluation goals.

LIMIT OF ERROR.

1. The boundaries within which the value of the attribute being determined lies with a specified probability. NOTE: The boundaries are defined to be plus or minus twice the standard deviation of the measured set, unless otherwise stipulated.
2. The uncertainties used in constructing a 95 percent confident interval associated with a quantity after any recognized bias has been eliminated or its effect accounted for. (Nuclear Material Control and Accountability)

LINE MANAGEMENT. DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

LINE SUPERVISION. The process of monitoring the communication link to ensure that it is operating correctly and that data have not been altered during transmission. (Physical Protection)

LIVE-ROUND EXCLUDER. A removable (spring pressure retained) flagging device inserted between the breech and the bolt face of a firearm which prevents a live round of ammunition from feeding from a magazine into the chamber without removal of the device.

LIVE-ROUND INHIBITOR. An obstructive device mounted in the cylinder or barrel of a firearm permitting chambering of blank ammunition but preventing the chambering of a live round or removal of the device.

LOCAL AREA NETWORK MATERIAL ACCOUNTING SYSTEM (LANMAS). A facility core nuclear materials accounting software product developed by the Department to enhance and support standardized nuclear materials accounting.

LOCAL CLASSIFICATION GUIDE. Classification guidance that is based on DOE Headquarters guidance and is tailored to apply to a specific facility or activity.

LOCAL THREAT ASSESSMENT. A threat assessment for a specific facility or operation.

LOSS.

1. The inability to locate classified matter, special nuclear material, or other Departmental interest. (See also DIVERSION AND THEFT.)
2. A positive inventory difference (ID) in the nuclear material inventory showing the book inventory to be greater than the physical inventory.

LOSS DETECTION ELEMENT. Any component of the safeguards system that can indicate an anomalous activity involving the possible loss of special nuclear material. (Nuclear Material Control & Accountability)

LOSS-OF-VIDEO ALARM. A feature built into a closed-circuit television camera system that annunciates when the picture is lost or has degraded to the point that the operator cannot identify objects within the camera's field of view.

LOW ENRICHED URANIUM. Uranium enriched below 20 percent in the isotope uranium-235.

LOW-LEVEL WASTE. Radioactive material that is not high-level radioactive waste, spent nuclear fuel, transuranic waste, or byproduct material as defined in 42 U.S.C. 2014 (Section 11, as amended, of the Atomic Energy Act of 1954), or that the U.S. Nuclear Regulatory Commission, consistent with existing law, classifies as low-level radioactive waste. (42 U.S.C. 10101, *Nuclear Waste Policy Act of 1982*)

LOW-READY. The position of a shooter holding a firearm with its muzzle (or a flashlight with its lens) pointed toward the ground and down-range, and below the line of a projectile's trajectory to a potential target.

LOW-TECHNOLOGY NUCLEAR EXPLOSIVE. A simulated nuclear explosive device or design which is made by an official Government program for research or training purposes concerning the improvised nuclear device problem. Does not include U.S. nuclear weapons or nuclear test devices.

M

91-B MATERIAL. Nuclear material transfers to the Department of Defense for use in national defense as directed by the President. (Nuclear Materials Management and Safeguards System)

91-C MATERIAL. Nuclear material transfers to another nation by sale, lease, or loan for military applications as authorized by the President. (Nuclear Materials Management and Safeguards System)

"M" MATERIALS. Usable excess nuclear material in a form suitable for direct introduction into production processes for which the Office of Weapons and Materials Planning has management responsibility.

MANAGED ACCESS. Under a variety of treaties, the process of negotiating inspection team access to places, objects, activities, or information, as necessary, to protect and prevent disclosure of classified or unclassified controlled information. The inspected state party must make every reasonable effort to demonstrate, through alternative means, that the place, object, activity, or information that is protected and to which access is managed is unrelated to the inspection mandate.

MATERIAL. Any substance regardless of its physical or chemical form. It includes raw, in-process, or manufactured commodity, equipment, component, accessory, part, assembly, or product of any kind. (Nuclear Material Control & Accountability)

MATERIAL ACCESS AREA (MAA). A type of security area that is approved for use, processing, and/or storage of a Category I quantity or other quantities of special nuclear material that can credibly roll-up to a Category I quantity and which has specifically defined physical barriers, is located within a protected area, and is subject to specific access controls.

MATERIAL BALANCE. A calculation evaluating the physical inventory of nuclear material actually present in an area using beginning and ending inventories after considering transfers of nuclear material into and out of the material balance area.

MATERIAL BALANCE AREA (MBA). An area that is both a subsidiary account of materials at a facility and a single geographical area that has defined boundaries and is an integral operation. It is used to identify the location and quantity of nuclear materials in the facility. (Nuclear Material Control & Accountability)

MATERIAL CONTAINMENT. A documented program designed to assure that nuclear materials are used, processed, or stored only with authorized security areas, storage repositories, and processing areas, and to detect unauthorized movement of materials across security boundaries. (Nuclear Material Control & Accountability)

MATERIAL CONTROL AND ACCOUNTABILITY ALARM.

1. General.
    a. Alarm from loss detection elements (e.g., special nuclear material monitors, material surveillance) which may indicate an abnormal situation and/or unauthorized use/removal of nuclear material.
    b. Alarm resulting from material control indicators (e.g., shipper/receiver difference, inventory difference, normal operating loss) exceeding established control limits.
2. Specific. A situation in which there is:
    a. an out-of-location item or an item whose integrity has been violated,
    b. an indication of a flow of strategic special nuclear material where there should be none, or
    c. a difference between a measured or observed amount or property of material and its corresponding predicted or property value that exceeds a threshold established to provide a detection capability. (10 CFR 74.4, *Definitions*) (Nuclear Material Control & Accountability)

MATERIAL CONTROL AND ACCOUNTABILITY (MC&A). Those parts of the safeguards program designed to provide information on, control of, and assurance of the presence of nuclear materials, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures. (Nuclear Material Control & Accountability)

MATERIAL CONTROL AND ACCOUNTABILITY PLAN. A documented description of a site or facility's material control and accountability program. (Nuclear Material Control & Accountability)

MATERIAL CONTROL INDICATORS. The discrepancy indicators provided by the accounting system that signify abnormal conditions. (Nuclear Material Control & Accountability)

MATERIAL CONTROL TEST. A comparison of a pre-established alarm threshold with the results of a process difference or process yield performed on a unit process. (Nuclear Material Control & Accountability)

MATERIALS MANAGEMENT PLAN. A planning document prepared annually that provides analyses of nuclear materials supply and demand requirements and related materials management issues for the current fiscal year plus the following 11-year planning period to support the Department, the Department of Defense, and other nuclear programs.

MATERIALS MANAGEMENT REVIEW OR APPRAISAL. The activities undertaken to evaluate the effectiveness of the materials management program, including established policies, procedures, and performance of nuclear materials management functions, and the identification of actions necessary to improve the program.

MATERIALS TRANSACTIONS.

1. Withdrawal: The receipt of nuclear material by a user project from a supply project.
2. Return: The removal of nuclear material from a user project to a supply project.
3. Transfer In: The receipt of nuclear material by a user project from any source other than a supply project.
4. Transfer Out: The removal of nuclear material from a user project to any destination other than a supply project.

MATERIAL SURVEILLANCE. The collection of information through devices and/or personal observation to detect unauthorized movements of nuclear material, tampering with nuclear material containers, falsification of information related to location or quantities of nuclear material, and tampering with safeguards devices.

MATERIAL SURVEILLANCE PROCEDURES. The instructions to ensure that nuclear materials are in their authorized location; detect unauthorized activities or anomalous conditions; and report material status. Examples include automated systems such as monitoring devices, sensors or other instrumentation; and visual surveillance/direct observation such as two-man rule, monitoring by external personnel or other alternative safeguards measures to detect the unauthorized removal or diversion of special nuclear material or an act of sabotage involving special nuclear material.

MATTER. Any combination of documents or material, regardless of physical form or characteristics.

MEASURAND. A particular quantity subject to measurement. The specification of a measurand may require statements about quantities such as time, temperature, and pressure.

MEASURED DISCARD. Nuclear material which has been measured, or estimated on the basis of measurements, and disposed of in such a way that it is not suitable for further nuclear use. (See also NORMAL OPERATIONAL LOSSES.)

MEASURED VALUE. The result of a measurement and its associated uncertainty.

MEASUREMENT. The determination of mass, volume, quantity, composition, or other property of a material where such determination is used for special nuclear material control and accounting purposes. (Based on 10 CFR 74.4, *Definitions*) (Nuclear Material Control & Accountability)

MEASUREMENT CONTROL. The procedures and activities used to:

1. ensure that a measurement process generates measurements of sufficient quality for their intended uses, or
2. obtain precision and accuracy values for use in MC&A.

MEASUREMENT ERROR. (See MEASUREMENT UNCERTAINTY.) (Nuclear Material Control & Accountability)

MEASUREMENT SYSTEM. All of the apparatus, equipment, instruments, and procedures used to perform a measurement.

MEASUREMENT UNCERTAINTY. (Nuclear Material Control & Accountability)

1. The parameter associated with the result of a measurement that characterizes the dispersion of the values that could reasonably be attributed to the measurand.
2. An estimate of the potential inaccuracies in a measured or derived quantity based on evaluation and combination of contributing sources of error.

MIXED OXIDE FUEL (MOX). A blend of plutonium and uranium oxides used as a fuel for nuclear power plants. A typical composition is 7 percent plutonium (PuO_2) mixed with depleted uranium (UO_2) to form MOX.

MODE. A masking state that applies to sensors or alarm groups. The values are "secure," "access," and "maintenance."

MODE CONTROL. The ability to change the mode of a sensor or alarm group.

MONITORING. The near-real-time collection and analysis of information about system behavior, such as throughput or performance. (Nuclear Material Control & Accountability)

MULTIPLE INTEGRATED LASER ENGAGEMENT SYSTEM (MILES). Equipment consisting of weapons-mounted laser transmitters and laser sensors that are mounted on potential targets (e.g., personnel, vehicles, buildings) to enable accurate assessment of the effects of weapons fire during simulated hostile engagements.

MUTUAL DEFENSE AGREEMENT. An agreement for cooperation between the U.S. and another nation for the exchange of nuclear weapon information and/or materials entered into pursuant to 42 U.S.C. 2153 (Section 123, as amended, of the Atomic Energy Act of 1954).

N

NATIONAL DEFENSE AREA. An area established on non-Federal lands located within the United States, its possessions, or territories for the purpose of protecting classified information or Department of Defense equipment and/or material.

NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP). A program established by Executive Order 12829, *National Industrial Security Program,* for the protection of classified information in the possession of a Government contractor.

NATIONAL SECURITY AREA. An area established on non-Federal lands located within the United States, its possessions, or its territories for the purpose of protecting classified information or Departmental equipment and/or material. The establishment of a National Security Area temporarily places such non-Federal lands under the effective control of the Department and results only from an emergency event

NATIONAL SECURITY ASSETS. The Departmental and contractor assets that require significant protection. These assets are nuclear weapons and their design, Category I and II quantities of special nuclear material, classified information, unclassified controlled information, critical facilities, and valuable Government property.

NATIONAL SECURITY AUTHORITY. An official of a North Atlantic Treaty Organization (NATO) member nation who is responsible for the security of NATO classified information within his or her country and its agencies abroad. The Secretary of Defense is the United States National Security Authority. The Assistant Deputy Under Secretary of Defense (Security Policy) has been appointed the United States Security Authority for NATO Affairs.

NATIONAL SECURITY INFORMATION (NSI). Any information that has been determined, pursuant to Executive Order 12958, *Classified National Security Information,* as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated.

NATIONAL TRAINING CENTER (NTC). A DOE organization comprised of multiple training academies and programs that support the development and implementation of centralized, standardized training, curriculum development, and other training-related services. The NTC provides the infrastructure in support of these academies and programs.

NAVAL NUCLEAR PROPULSION INFORMATION (NNPI). Information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of Naval nuclear-powered ships and prototypes, including the associated nuclear support facilities.

NEAR-SITE BOUNDARY. The site boundary closest to the target/asset.

NEED-TO-KNOW. A determination made by an authorized holder of classified or unclassified controlled information that a prospective recipient requires access to specific classified or unclassified controlled information in order to perform or assist in a lawful and authorized Governmental function.

NERVE AGENT. A chemical agent that acts by disrupting the normal functioning of the nervous system.

NONDESTRUCTIVE ANALYSIS. The measurement of material that is done without destroying the material and without changing its chemical or physical properties.

NORMAL (NATURAL) URANIUM. Uranium as found in nature, containing about 0.7 percent uranium-235, 99.3 percent uranium-238, and a trace of uranium-234. The natural

isotopic composition varies slightly world-wide. The United States defines normal uranium as that containing 0.711 percent uranium-235 by weight.

NORMAL OPERATIONAL LOSSES. Known quantities (by measurement or engineering estimate) of nuclear materials which have been separated from a process or operation as wastes during processing and disposed of by approved methods. (See also MEASURED DISCARD.) (Nuclear Material Control & Accountability)

NUCLEAR COMMAND AND CONTROL SYSTEM. The designated combination of flexible and enduring elements including facilities, equipment, communications, procedures, personnel, and the structure in which these elements are integrated, all of which are essential for planning, directing, and controlling nuclear weapon operations of military forces and the activities that support those operations.

NUCLEAR COMPONENTS. Those parts of a nuclear explosive or special assembly, or test parts or subassembly, that contain fissile and/or radioactive and other materials.

NUCLEAR DEVICE. A collective term for a nuclear explosives device, including a nuclear weapon, a weapon prototype, or a weapon test device.

NUCLEAR EMERGENCY SUPPORT TEAM (NEST). A worldwide, deployable capability of specialized elements to deal with the technical aspects of nuclear and radiological terrorism.

NUCLEAR EXPLOSIVE-LIKE ASSEMBLY. An assembly that represents a nuclear explosive in its basic configuration (main charge high-explosive and pit) and any subsequent level of assembly up to its final configuration, or which represents a weaponized nuclear explosive such as a warhead, bomb, reentry vehicle, or artillery shell. A nuclear explosive-like assembly does not contain an arrangement of high-explosive and fissile material capable of producing a nuclear detonation.

NUCLEAR FACILITY. A facility for the production, use, storage, or handling of nuclear material, including irradiated material that is of national security significance.

NUCLEAR MATERIAL HOLDUP. (See HOLDUP.)

NUCLEAR MATERIALS.

1. All materials so designated by the Secretary of Energy. At present, these materials are depleted uranium, enriched uranium, americium-241, americium-243, curium, berkelium, californium-252, plutonium 238-242, lithium-6, uranium-233, normal uranium, neptunium-237, deuterium, tritium, and thorium.
2. Special nuclear material, byproduct material, or source material as defined in 42 U.S.C. 2014 (aa), (e), and (z) [Sections 11(aa), (e), and (z), respectively, of the Atomic Energy Act of 1954], or any other material used in the production, testing, use, or assembly of nuclear weapons or components of nuclear weapons that the Secretary of Energy determines to be nuclear material in accordance with 10 CFR 1017.10(a).

NUCLEAR MATERIALS ACCOUNTABILITY. (See also ACCOUNTABILITY.) The part of the Material Control and Accountability program encompassing the procedures and systems to:

1. perform nuclear material measurements,
2. verify the locations and quantities of nuclear materials through physical inventories,
3. maintain records and provide reports,
4. perform data analyses to account for nuclear material and to detect losses, and
5. investigate and resolve apparent losses of nuclear material.

NUCLEAR MATERIALS ACCOUNTING. The principles and/or practices of systematically recording, reporting, and interpreting nuclear material transaction and physical inventory data.

NUCLEAR MATERIALS CATEGORY. A designation of nuclear material defined by the type of material and quantity present, which establishes the level of protection required for that material.

NUCLEAR MATERIALS CONTROL. The part of the safeguards program encompassing management and process controls to:

1. assign and exercise responsibility for nuclear materials;
2. maintain vigilance over the materials;
3. govern movement, location, and use of the materials;
4. monitor inventory and process status;
5. detect unauthorized activities for all nuclear materials; and
6. help to investigate and resolve apparent losses of nuclear materials.

NUCLEAR MATERIALS COURIER. A Q-cleared Office of Secure Transportation Federal agent who has been authorized under 42 U.S.C. 220(k) [Section 161(k), as amended, of the Atomic Energy Act of 1954] to carry firearms and make arrests without warrant and who is charged with the responsibility of safely and securely transporting and/or escorting nuclear devices, nuclear components, and sensitive nuclear materials when assigned by the Transportation Safeguards System. When so assigned, the courier is authorized under 10 CFR 1047.7(a)(3) and (4) to use deadly force to protect certain items.

NUCLEAR MATERIALS CUSTODIAN (NMC). An individual assigned responsibility for the control of nuclear material in a localized area of a facility (e.g., a single material balance area). The NMC is responsible for keeping the nuclear materials representative apprised of activities within the facility.

NUCLEAR MATERIALS INSPECTION/SURVEY. A comprehensive examination and evaluation of the effectiveness of the control and accountability systems for nuclear materials at a Departmental facility.

NUCLEAR MATERIALS MANAGEMENT AND SAFEGUARDS SYSTEM (NMMSS). The national database and information system for nuclear materials controlled by the Government, created to support national safeguards and management objectives in the domestic and foreign use of nuclear resources.

NUCLEAR MATERIALS REPRESENTATIVE (NMR). The individual at a facility responsible for nuclear materials reporting and data submission to the Nuclear Materials Management and Safeguards System. Also called the Nuclear Materials Account Representative (NMAR).

NUCLEAR THREAT MESSAGE. A communication that provides information concerning the intent to commit (or refers to the committing of) a nuclear-related malevolent act. The threatened malevolent act could be a nuclear explosion, contamination of a large populated area by dispersal of radioactive material, or sabotage of a nuclear facility, site, or system.

NUCLEAR WEAPON ACCIDENT. An unexpected event involving nuclear weapons or nuclear components that results in any of the following:

1. accidental or unauthorized launching, firing, or use by U.S. forces or U.S.-supported allied forces of a nuclear-capable weapon system;
2. accidental, unauthorized, or unexplained nuclear detonation;
3. non-nuclear detonation or burning of a nuclear weapon or nuclear component;
4. radioactive contamination;
5. jettisoning of a nuclear weapon or nuclear component; or
6. public hazard, actual or perceived.

NUCLEAR WEAPON INCIDENT. An unexpected event, including acts of nature, involving a nuclear weapon, facility, or component resulting in any of the following, but not constituting a nuclear weapons accident:

1. an increase in the possibility of explosion or radioactive contamination;
2. errors committed in the assembly, testing, loading, or transportation of equipment and/or the malfunctioning of equipment and material which could lead to an unintentional operation of all or part of the weapon arming and/or firing sequence or which could lead to a substantial change in yield or increased dud probability; or
3. damage to a weapon, facility, or component.

NUCLEAR WEAPON STATE. Any country that manufactured and detonated a nuclear weapon or other explosive device before January 1, 1967, as recognized by the Nuclear Non-Proliferation Treaty. Refers to China, France, Russia (as the successor to the Soviet Union), the United Kingdom, and the United States.

NUCLEAR WEAPON SURETY. The safety, security, use control, and effectiveness of nuclear weapons.

NUISANCE ALARM. The alarm produced by an intrusion detection sensor in response to a known stimulus (e.g., wind, lightning, thunder, accident) unrelated to an intrusion attempt.

O

OBLIGATIONS TRACKING. The tracking of transfers of nuclear material that have been identified as having a foreign accounting obligation attached based on one or more Agreements for Cooperation in the Peaceful Uses of Atomic Energy. (Nuclear Material Control & Accountability)

OBSERVATION FLIGHT. The flight of the observation aircraft conducted by the observing party over the territory of the observed party, as provided in the flight plan, from the point of entry or Treaty on Open Skies airfield to the point of exit or Treaty on Open Skies airfield.

OCCURRENCE. One or more (i.e., recurring) events or conditions that adversely affect, or may adversely affect, DOE or contractor personnel, the public, property, the environment, or the DOE mission. Events or conditions meeting the criteria thresholds identified in DOE M 231.1-2 or determined to be recurring through performance analysis are occurrences.

OFFENSIVE COMBATIVE PERSONNEL. Security police officers assigned to response force duties including pursuit and assault functions.

OFFICIAL USE ONLY.

1. A designation used by DOE to identify certain unclassified controlled information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552).
2. A security classification marking used during the period July 18, 1949, through October 22, 1951.

OFFSITE. The areas outside the boundaries and jurisdiction of a Departmental facility.

ONSITE. An area within the boundaries and/or Departmental control to which the public does not have free and uncontrolled access.

ONSITE INSPECTION. Physical presence of inspectors at facilities subject to verification activities, and the exercise of inspector access to facilities/sites for the purposes of collecting treaty-related information.

OPEN STORAGE. The storage of classified matter within a secure storage repository (e.g., vault, vault-type room) in a manner such that a person could view the material if he/she has access to the room.

OPERABILITY TEST. A test to confirm, without any indication of effectiveness, that a system element or total system is operating.

OPERATIONS SECURITY (OPSEC). A process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the inadvertent disclosure of such information.

ORIGINAL CLASSIFICATION. A determination by an Original Classifier that certain new information requires protection against unauthorized disclosure because of national security interests under Executive Order 12958, *Classified National Security Information,* as amended. Such information is identified as National Security Information.

ORIGINAL CLASSIFIER. A Federal employee who is authorized to determine under Executive Order 12958, *Classified National Security Information,* as amended, that certain new information requires protection against unauthorized disclosure in the interest of national security; such information is identified as National Security Information.

OUTSIDER. A person who does not have official business with the Department and has not been granted routine access to a Departmental program, operation, facility, or site.

OVERFLIGHT. A confidence-building measure or other form of arms control verification permitted by certain treaties such as the Treaty on Open Skies, Chemical Weapons Convention, and Comprehensive Nuclear Test-Ban Treaty, under circumstances specified in each treaty.

P

PANIC HARDWARE. A door-locking mechanism that is always operable from inside the building by pressure on a crash bar or lever.

PASSIVE BARRIER. An obstruction to passage which, by its nature, impedes or deters entry or exit (e.g., a wall, ceiling, floor, or fence).

PERFORMANCE ASSURANCE. Demonstration of the adequacy of S&S systems to meet protection needs by means of systematic evaluation of procedures, administrative operations, integrated systems, hardware, software, protective personnel, and other staff.

PERFORMANCE ASSURANCE PROGRAM. A Departmental S&S program used to assess the effectiveness of the protection provided safeguards and security interests by systematically evaluating all protection programs' essential elements implemented to comply with Departmental directives' requirements.

PERFORMANCE TEST (PT). A test to evaluate the ability of an implemented and operating system element or total system to meet an established requirement.

PERIMETER.

1. The outer boundary of an area, which may be designated by a fence or wall.
2. The conceptual limit that encompasses all components of a classified automated information system to be accredited by the designated accrediting authority.

3. (Under treaties and agreements) The external boundary of the inspection site.

PERIMETER INTRUSION DETECTION AND ASSESSMENT SYSTEM (PIDAS). A mutually supporting combination of barriers, clear zones, lighting, and electronic intrusion detection, assessment, and access control systems constituting the perimeter of the protected area and designed to detect, impede, control, or deny access to the protected area.

PERMISSIVE ACTION LINK (PAL). A device included in or attached to a nuclear weapon system to preclude arming and/or launching until the insertion of a prescribed discrete code or combination. It may include equipment and cabling external to the weapon or weapon system to activate components within the weapon or weapon system.

PERSONAL ELECTRONIC DEVICE (PED). A generic term for small, transportable electronic items that are equipped with the capabilities to process, store, transmit, receive, and/or manipulate electronic data.

PERSONALLY OWNED EQUIPMENT/PROPERTY. Items not owned by the Government and not permanently affixed to, or a part of, the real estate. Generally, items remain personal property if they can be removed without serious damage either to the real property or to the items themselves.

PERSONNEL SECURITY/PERSONNEL SECURITY PROGRAM. A defined set of policies, procedures, and activities established to ensure that granting an individual access to classified matter and/or special nuclear material would not endanger the common defense and security and would be clearly consistent with the national interest.

PERSONNEL SECURITY CLEARANCE. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted. (National Industrial Security Program Operating Manual) (See also ACCESS AUTHORIZATION.)

PHYSICAL INVENTORY.

1. The quantity of nuclear material which is determined to be on hand by physically ascertaining its presence using techniques such as sampling, weighing, and analysis.
2. The act of quantifying nuclear material that is on hand by physically ascertaining its presence using techniques such as electronic or visual verification, sampling, weighing, and analysis.
3. A determination on a measured basis of the quantity of nuclear material on hand at a given time. The methods of physical inventory and associated measurements vary depending on the material to be inventoried and the process involved. (Nuclear Material Control & Accountability)

PHYSICAL PROTECTION. The application of physical or technical methods designed to protect personnel; prevent or detect unauthorized access to facilities, material, and documents; protect against espionage, sabotage, damage, and theft; and respond to any such acts should they occur.

PIGGYBACKING. Entering a security area with or behind a cleared authorized person who has vouched for the accompanying individual's authorization for access. (See also VOUCHING.)

PIT (LIVE). A fissile component, or set of fissile components, designed to fit in the central cavity of an implosion system and which if placed there will create a nuclear explosive.

POINT OF ENTRY/POINT OF EXIT (POE). The location designated by the observed or inspected country for the in-country arrival/departure of inspection or observation teams.

PORTAL MONITOR.

1. Any electronic instrument designed to perform scans of items, personnel, and vehicles entering or leaving a designated area for the purpose of detecting controlled or prohibited articles such as weapons, explosives, and nuclear material.
2. A designated point consisting of systems and protective personnel designed to scan items, personnel, and vehicles for the purpose of detecting controlled and prohibited articles.

PORTION MARKING. The application of certain classification and control markings to individual words, phrases, sentences, or paragraphs of a classified document to indicate their specific classification level and category (if Restricted Data or Formerly Restricted Data) or control category (e.g., Unclassified Controlled Nuclear Information, Official Use Only).

POSITIVE MEASURES. The combination of procedural and administrative actions, physical safeguards, and features expressly designed for the purpose of ensuring security, safety, and control of nuclear weapons and systems, including associated personnel.

POST ORDER. The written operational requirements for a designated protective force post.

POTENTIAL COMPROMISE. An event where circumstances exist such that the compromise of classified information cannot be ruled out.

PRACTICABLY IRRECOVERABLE. A characteristic of waste which makes the contained nuclear materials not recoverable due to economic and/or technology limitations.

PRECISION. A quantitative measure of the variability of a set of repeated measurements under a prescribed set of conditions. (Nuclear Material Control & Accountability)

PRECISION RIFLEMAN/FORWARD OBSERVER TEAM (PRFOT). Selected individuals from a Special Response Team who have successfully completed approved precision rifle qualification and are capable of providing accurate long range fire.

PRELIMINARY INQUIRY. A review of the circumstances surrounding a suspected or alleged incident of security concern to discover all factual information related to the incident.

PRIMARY STANDARD. A standard that is designated or widely acknowledged as having the highest metrological qualities and whose value is accepted without reference to other standards of the same quantity. (Nuclear Material Control & Accountability)

PROBABILITY OF DETECTION (P_D). The likelihood of a detection element of a physical security system (e.g., sensor, security police officer, etc.) to recognize an external stimulus as an adversarial action within a specific zone of coverage.

PROCESS DIFFERENCE. The determination of an inventory difference on a unit process level with the additional qualification that difficult to measure components may be modeled. (10 CFR 74.4, *Definitions*)

PRODUCE. In relation to special nuclear material, to:

1. manufacture, make, or refine special nuclear material;
2. separate special nuclear material from other substances in which such material may be contained; or
3. make new special nuclear material.

PROHIBITED ARTICLES. Any item administratively restricted from being introduced into a security area

PROJECT NUMBER. A 10-character alphanumeric description that identifies nuclear materials allocated for tasks or phases of work. NOTE: Project numbers generally are derived from the DOE Budget and Reporting Classification System. (Nuclear Material Control & Accountability)

PROPERTY PROTECTION AREA (PPA). A type of security area having defined boundaries and access controls for the protection of Departmental property.

PROPERTY PROTECTION FACILITY. A facility where the program office has determined that a special standard of protection must be applied. For example, such a facility may have property of significant monetary value (i.e., more than $5,000,000); nuclear materials requiring safeguards controls or special accounting procedures; property of significance to Departmental program continuity or national security considerations; or property that, if mishandled, could have adverse impacts upon the public health and safety.

PROTECTED AREA (PA). A type of security area defined by physical barriers (i.e., walls or fences) and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II special nuclear material and classified matter and/or to provide a concentric security zone surrounding a material access area or a vital area.

PROTECTED DISTRIBUTION SYSTEM (PDS). A wireline or fiber optic telecommunications system that includes adequate acoustical, electrical, electromagnetic, and physical security measures to permit its use for the transmission of unencrypted classified information.

PROTECTION PROGRAM. The Departmental activities that protect Departmental property and personnel from adversary actions that would have an adverse impact on the national security, the health and safety of employees, the public, or the environment.

PROTECTION STRATEGIES. Technical and tactical techniques to mitigate the design basis threats against special nuclear material, vital equipment, classified matter, and other Departmental property. The strategies are for the protection of Departmental property from adversary actions that would impact the national security, the health and safety of employees, the public, or the environment.

PROTECTIVE FORCE (PF). Those Federal or contractor personnel assigned to protective duties involving the S&S interests of the Department.

PROTECTIVE FORCE OFFICER. As defined in 10 CFR 1047.3(g), any person authorized by the Department to carry firearms under 42 U.S.C. 2201(k) [Section 161(k), as amended, of the Atomic Energy Act of 1954].

PROTECTIVE PERSONNEL. Security officers, security police officers, Office of Secure Transportation Federal agents (i.e., nuclear materials couriers), Federal officers, and Office of Special Operations special agents assigned to details, who are employed to protect safeguards and security interests.

PROTRACTED THEFT OR DIVERSION. Theft or diversion that is accomplished by repeated occurrences.

Q

Q ACCESS AUTHORIZATION. A type of authorization granted by the Department indicating that the recipient is approved for access to the following levels of classified matter on a need-to-know basis: Top Secret, Secret, and Confidential Restricted Data, National Security Information, and Formerly Restricted Data.

R

RADIATION EXPOSURE DEVICE (RED). A device that is intended to expose people to radiation without dispersal of radioactive material into the air by detonation with conventional explosives or other means. An example of a RED is unshielded or partially shielded radioactive materials placed in any type of container and in a location capable of causing a radiation exposure to one or more individuals.

RADIOACTIVE DECAY. The decrease in activity of any radioactive material with the passage of time due to spontaneous emission from the atomic nuclei of either alpha or beta particles, sometimes accompanied by gamma radiation. X-rays may also be emitted following orbital electron capture. Certain nuclei may also undergo spontaneous fission.

RADIO DISCIPLINE. Minimizing transmission time by limiting the number and length of transmissions and communications to only mission-essential items.

RADIOLOGICAL DISPERSAL DEVICE (RDD). A device or mechanism that is intended to spread radioactive material from the detonation of conventional explosives or other means.

RADIOLOGICAL INCIDENT. An incident during which personnel or the environment receive an exposure to radiation as a result of an accident or an act of sabotage.

RANDOM ERROR. The chance variation encountered in all measurement work characterized by the random occurrence of both positive and negative deviations from the mean value. (ASTM C1215-92(1997), *Standard Guide for Preparing and Interpreting Precision and Bias Statements in Test Method Standards Used in the Nuclear Industry*)

RANDOM PATROL. A patrol conducted in a manner such that the location of the patrol at any specific time cannot be predicted.

RANGE MASTER. The individual designated to provide overall management and administration of a live-fire range facility to ensure that all operations and training are conducted in accordance with applicable Departmental directives.

RANGE SAFETY OFFICER. The designated and specifically trained individual responsible for safety at a live fire range.

RECAPTURE. Regaining control of a nuclear weapon and/or special nuclear material, which is under unauthorized possession, while still within the confines of a Departmental site/facility.

RECLASSIFICATION. A determination by an appropriate authority that restores the classification to (1) information that was classified as National Security Information and then declassified or (2) matter that was classified as Restricted Data, Formerly Restricted Data, or National Security Information, and then erroneously declassified.

RECOVERY. Regaining control of a nuclear weapon and/or special nuclear material, which is under unauthorized possession and has been removed from within the confines of a Departmental site/facility or Departmental possession.

REDACTION. The removal of classified or unclassified controlled information from a document.

RED/BLACK CONCEPT. The separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

REFERENCE MATERIAL. A material or substance, one or more of whose property values are sufficiently homogeneous and well established to be used for the calibration of an apparatus, the assessment of a measurement method, or the assignment of values to materials. (Nuclear Material Control & Accountability)

REFERENCE STANDARD. A material, device, or instrument whose assigned value is known relative to national standards or nationally accepted measurement systems. This is also commonly called a traceable standard. (10 CFR 74.4, *Definitions*) (Nuclear Material Control & Accountability)

REFRESHER BRIEFING. An annual briefing for access authorization holders to reinforce information provided in the comprehensive briefing, and to address current S&S and counterintelligence awareness issues.

REPEATABILITY (OF MEASUREMENT RESULTS). The closeness of the agreement between the results of successive measurements of the same measurand carried out under the same conditions of measurement. Repeatability conditions include the same measurement procedure, the same observer, and the same measuring instrument, used under the same conditions; the same location; and repetition over a short period of time. Repeatability may be expressed quantitatively in terms of the dispersion characteristics of the results.

REPORTABLE QUANTITY OF NUCLEAR MATERIAL. The quantity of nuclear material required to be reported to the NMMSS. (See DOE M 470.4-6, *Nuclear Material Control and Accountability*.) For example, the reportable quantity of depleted uranium is 1 kilogram, but for plutonium, the reportable quantity is 1 gram.

REPORTING IDENTIFICATION SYMBOL (RIS). A unique combination of three or four letters assigned to each reporting organization by DOE or the Nuclear Regulatory Commission for the purpose of identification in the Nuclear Material Management and Safeguards System database.

REPRODUCIBILITY (OF MEASUREMENT RESULTS). The closeness of the agreement between the results of measurements of the same measurand carried out under changed conditions of measurements. A valid statement of reproducibility requires specification of the conditions changed. The changed conditions may include principle of measurement, measurement method, observer, measuring instrument, reference standard, location, conditions of use, and time. Reproducibility may be expressed quantitatively in terms of the dispersion characteristics of the results.

RESIDUAL RISK. The portion of risk remaining after security measures have been applied.

RESPONSE FORCE. Protective force; special response team; and Federal, State, and local law enforcement agency personnel.

RESTRICTED.

1. A former U.S. security classification marking used before December 15, 1953.
2. An active security classification marking used by some foreign governments and international organizations.

RESTRICTED DATA (RD). All data concerning design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy, but excluding data declassified or removed from the Restricted Data category pursuant to 42 U.S.C. 2162 [Section 142, as amended, of the Atomic Energy Act of 1954].

RETAINED WASTE. The nuclear material generated from processing or from an operational accident, which is deemed to be unrecoverable for the time being but which is stored. (See also PRACTICABLY IRRECOVERABLE.)

RISK. The qualitative or quantitative expression of possible loss that considers both the likelihood that an event will occur and the consequence of that event.

RISK ANALYSIS. An analysis of safeguards and/or security system assets and vulnerabilities to establish an expected loss from certain events.

RISK ASSESSMENT. An evaluation of potential threats against a safeguards and security interest and the countermeasures necessary to address potential vulnerabilities. It is a five-step process that provides the decision-maker with a firm foundation upon which to make an informed decision. During a risk assessment, the value of the information, analysis of the threat, and determination of the information's vulnerability are conducted. Following the completion of these three activities, a determination of the risk rating is made and countermeasures are considered and implemented, as necessary.

RISK MANAGEMENT. The integrated process of assessing the threat, the vulnerabilities, and the value of the asset, and applying cost-effective countermeasures.

ROBUSTNESS. The insensitivity of a measurement method to moderate changes in measurement parameters. If changes in a parameter significantly increase the imprecision of a measurement, the permitted operating range of a measurement system may be restricted. Robustness studies rapidly identify significant sources of measurement uncertainty. (Nuclear Material Control & Accountability)

ROLLING. Entering and leaving the detection zone lying on the ground and rotating one's body about its long axis at an approximate velocity of 0.1 meter per second while maintaining a low profile.

ROLL-UP. The accumulation of smaller quantities of special nuclear material to a higher category, based upon a compliance standard using the Graded Safeguards Table (DOE M 470.4-6, *Nuclear Material Control and Accountability*). (See also CREDIBLE ROLL-UP.) (Nuclear Material Control & Accountability)

S

SAFEGUARDING. Measures and controls that are prescribed to protect classified information and matter. (Executive Order 12958, *Classified National Security Information*, as amended)

SAFEGUARDS. An integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of nuclear materials.

SAFEGUARDS AND SECURITY ACTIVITY. Any work performed under contract, subcontract, or other agreement which involves access to classified information, nuclear material, or Departmental property of significant monetary value by the Department, a Departmental contractor, or any other activity under the Department's jurisdiction. Also included is the verification of the capabilities of approved Federal locations.

SAFEGUARDS AND SECURITY ALARM MANAGEMENT AND CONTROL SYSTEM FOR HIGH-CONSEQUENCE APPLICATIONS. A functional description which establishes the Department's integrated security system requirements for compliance with Departmental requirements for upgrades of existing systems and design/installations of new systems.

SAFEGUARDS AND SECURITY INFORMATION MANAGEMENT SYSTEM (SSIMS). An automated information system used to record facility approvals, facility administrative information, survey and inspection findings, and corrective actions.

SAFEGUARDS AND SECURITY INTEREST. A general term for any Departmental resource or property that requires protection from malevolent acts. It may include but is not limited to classified matter, special nuclear material and other nuclear materials, secure communications centers, sensitive compartmented information facilities, automated data processing centers, facilities storing and transmitting classified information, vital equipment, or other Departmental property.

SAFEGUARDS AND SECURITY SURVEY. A performance- and compliance-based examination and evaluation of the effectiveness of the implementation of a security program.

SAFEGUARDS TRANSPORTER (SGT). The trailer used to transport special nuclear material. NOTE: SGTs are the replacements for safe secure trailers, some of which are still in operation.

SAFE HAVEN. The temporary storage provided for Office of Secure Transportation convoys at Department of Defense facilities in order to ensure safety and security of nuclear material and/or non-nuclear classified material during civil disturbances, natural disasters, and/or other conditions which could affect the safety or security of the Departmental shipment.

SAFE SECURE TRAILER (SST). A modified semi-trailer which is used for highway transport of special nuclear material, including nuclear weapons.

SAFETY ANALYSIS REPORT (SAR). A report summarizing the hazards associated with the operation of a particular facility or activity and defining minimum safety requirements.

SAFETY BAFFLES. Vertical or sloping barriers designed to prevent a projectile from traveling into an undesired area or direction, most often used to prevent bullets from leaving a live-fire range proper.

SCRAP.

1. The by-products from chemical and/or mechanical processing, not usable in their present forms, from which nuclear materials can be economically recovered.
2. The various forms of special nuclear material generated during chemical and mechanical processing, other than recycle material and normal process intermediates, which are unsuitable for continued processing, but all or part of which will be converted to useable material by appropriate recovery operations. (10 CFR 74.4, *Definitions*)

SEALED SOURCE. Radioactive material usually encased in metal or plastic that may present an external exposure hazard, but not a significant contamination hazard under normal conditions.

SECONDARY ALARM STATION (SAS). A continuously staffed location, physically separated from the Central Alarm Station, with the capability to provide alarm annunciation and response as a back-up to the Central Alarm Station, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.

SECONDARY STANDARD. A standard whose value is assigned by comparison with a primary standard of the same quantity. (Nuclear Material Control & Accountability)

SECRET. The classification level applied to information for which the unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

SECURE. The mode of a sensor or alarm group during which the physical state of the sensor or alarm group is passed on to the operator.

SECURE COMMUNICATIONS CENTER. An organization charged with the responsibility for receipt, transmission, and delivery of both classified and unclassified messages. It normally includes a distribution center, message center, cryptocenter, transmitting facilities, and receiving facilities, all of which are located in the security area.

SECURE STORAGE REPOSITORY. An approved storage facility for the protection of special nuclear material and/or classified matter (e.g., vault, vault-type room, General Services Administration-approved security container, and other selected secure storage containers).

SECURITY. An integrated system of activities, systems, programs, facilities, and policies for the protection of classified information and/or classified matter, unclassified controlled information, nuclear materials, nuclear weapons, nuclear weapon components, and/or the Department's and its contractors' facilities, property, and equipment.

SECURITY AREA. A defined area containing S&S interests that requires physical protection measures. The types of security areas used within the Department include property protection areas, limited areas, exclusion areas, protected areas, material access areas, vital areas, and functionally specialized security areas, such as sensitive compartmented information facilities, classified computer facilities, and secure communications centers.

SECURITY ASSURANCE. A written certification, from one government to another, of the security clearance level of its employees, contractors, and citizens.

SECURITY BADGE. A distinctive tag used for controlling access to facilities and security areas that provides an individual's name, photograph, and access authorization type and that may include additional information in electromagnetic, optical, or other form.

SECURITY CLEARANCE. An administrative determination by certain Federal agencies (other than DOE and NRC) that an individual is eligible for access to classified information. Security clearances are designated as Top Secret, Secret, or Confidential, indicating that the recipient is approved for access to National Security Information or Formerly Restricted Data at a classification level equal to or less than his/her security clearance level. (For DOE and NRC, see ACCESS AUTHORIZATION.)

SECURITY CONTAINER. A filing cabinet type of safe which bears a test certification label on the inside of the locking drawer or door and is marked "General Services Administration Approved Security Container" on the top or control drawer or door.

SECURITY INCIDENT. Actions, inactions, or events that have occurred that 1) pose threats to national security interests and/or Departmental property; 2) create potentially serious or dangerous security situations; 3) potentially endanger the health and safety of the workforce or public (excluding safety related items); 4) degrade the effectiveness of the S&S program, or 5) adversely impact the ability of organizations to protect S&S interests.

SECURITY INTEREST. (See SAFEGUARDS AND SECURITY INTEREST.)

SECURITY PLAN. An official document that describes the use of resources by a facility to protect the facility, its sites, and its assets from attack.

SECURITY SHIPMENT. A shipment between security areas and/or Departmental and non-Departmental facilities consisting of classified matter or special nuclear material.

SECURITY SURVEY. (See SAFEGUARDS AND SECURITY SURVEY.)

SECURITY SYSTEM. The combination of personnel, equipment, hardware and software, structures, plans and procedures, etc., that is used to protect S&S interests.

SECURITY THREAT. The technical and operational capability of an adversary to identify and to exploit vulnerabilities.

SELECTIVITY / SPECIFICITY. The degree to which a measurement method responds uniquely to the material of interest. (Nuclear Material Control & Accountability)

SENIOR AGENCY OFFICIAL. The official designated by the Federal agency head under Section 5.4 of Executive Order 12958, *Classified National Security Information*, as amended, to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

SENIOR CONTROLLER. An individual with overall responsibility for assigning tasks and coordinating the efforts of other functional element controllers during force-on-force exercises and other performance tests.

SENSITIVE COMPARTMENTED INFORMATION (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected in accordance with policy established by the Director, Central Intelligence.

SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF). An accredited area, room, group of rooms, or installations where Sensitive Compartmented Information may be stored, used, discussed, and/or electronically processed.

SENSITIVE NUCLEAR MATERIAL PRODUCTION INFORMATION. Any information involving classified production rate or stockpile quantity information relating to plutonium, tritium, enriched lithium-6 and uranium-235 and uranium-233, laser separation technology, classified gaseous diffusion technology, classified gas centrifuge technology, and classified advanced isotope separation technology.

SENSITIVITY. The change in the response of a measuring instrument divided by the corresponding change in the stimulus. The sensitivity may depend on the value of the stimulus. (Nuclear Material Control & Accountability)

SENSOR OR ALARM GROUP PHYSICAL STATE. The condition of a sensor or alarm group that is evaluated by Security Alarm Management and Control System. For digital sensors, the state can be "OK" or "detect" For supervised line point sensors, the value can be "OK," "detect," or "tamper." Analog sensors typically provide a voltage or current value.

SHADOW FORCE. An armed security force that provides continuing site protection under the constant supervision of a controller while an exercise is being conducted.

SHIELD. A metal (or other material), police-type badge imprinted with the name of the issuing authority and the serial number of the badge, which provides additional identification of the bearer.

SHIPPER/RECEIVER DIFFERENCE. The difference between the measured quantity of nuclear material stated by the shipper as having been shipped and the measured quantity stated by the receiver as having been received.

SHROUDING. The process of covering and/or concealing classified, unclassified controlled, or proprietary assets to protect them from visual observation.

SIGMA CATEGORIES. A Department term relating to Restricted Data and/or Formerly Restricted Data concerning the theory, design, manufacture, storage, characteristics, performance, effects, or use of nuclear weapons, nuclear weapon components, or nuclear explosive devices or materials.

SIGNIFICANT VULNERABILITY. The loss of, or discovered way to bypass, an essential S&S system component or set of components for which there is no effective back-up.

SIMPLE COMPOUNDS. One or more special nuclear materials combined essentially with one other element, for example, oxides, carbides, nitrates, and fluorides.

SINGLE-SCOPE BACKGROUND INVESTIGATION (SSBI). A background investigation consisting of record reviews and indices checks, a subject interview, and interviews with sources of information as specified in the "Investigative Standards for Background Investigations for Access to Classified Information," which implement Executive Order 12968. This type of investigation is used as a basis for initially determining an individual's eligibility for a Q access authorization, a Top Secret security clearance, or access to sensitive compartmented information.

SITE.

1. A geographical area where one or more facilities are located.
2. A geographical area consisting of a Departmental-controlled land area including Departmental-owned facilities (e.g., the Oak Ridge Reservation, the Nevada Test Site, and the Hanford Site).

SITE SAFEGUARDS AND SECURITY PLAN (SSSP). An official document required at facilities containing Category I SNM or with credible roll-up that describes the site-wide protection programs and evaluations of risk associated with DOE O 470.3, *Design Basis Threat Policy,* and identified facility targets.

SITE SECURITY PLAN (SSP). An official document that describes the protection program in place that is required at locations which, because of limited scope of interests, do not require an SSSP.

SITE SURVEY. The process of conducting a security evaluation of a building or outdoor area to be visited or reasonably expected to be used by the principal. (Executive Protection)

SOFTWARE CONFIGURATION MANAGEMENT. Configuration control of the software used in the system; e.g., keeping versions updated and maintaining older versions.

SOURCE DOCUMENT. A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

SOURCE MATERIAL. Depleted uranium, normal uranium, thorium, or any other nuclear material determined, pursuant to 42 U.S.C. 2091 (Section 61, as amended, of the Atomic Energy Act of 1954) to be source material or ores containing one or more of the foregoing materials in such concentration as may be determined by regulation.

SPECIAL ACCESS PROGRAM (SAP). A program established for a specific class of classified information that imposes protection and access requirements that exceed those normally required for information at the same classification level.

SPECIAL NUCLEAR MATERIAL (SNM). Plutonium, uranium-233, uranium enriched in the isotope 235, and any other material which, pursuant to 42 U.S.C. 2071 (Section 51, as amended, of the Atomic Energy Act of 1954), has been determined to be special nuclear material, but does not include source material; it also includes any material artificially enriched by any of the foregoing, not including source material.

SPECIAL RESPONSE TEAM (SRT). Security police officers, certified at Level III, trained and deployed as a unit and assigned to a site or facility, who have received special training to provide additional protection as demanded by particular targets, threats, and vulnerabilities existing at their location.

SPENT NUCLEAR FUEL (SPENT FUEL) (SNF). The fuel that has been withdrawn from a nuclear reactor following irradiation, the constituents of which have not been separated by reprocessing. (42 U.S.C. 10101, Nuclear Waste Policy Act of 1982)

STANDARD.

1. A rule or basis of comparison in measuring or judging capacity, quantity, content, extent, value, quality, etc.
2. A model, established by law, regulation, order, policy, custom, or general agreement, against which a security system can be measured.

STANDARD ERROR OF THE INVENTORY DIFFERENCE. The standard deviation of an inventory difference that takes into account all measurement error contributions to the components of the inventory difference. (10 CFR 74.4, *Definitions*)

STANDARD ERROR OF THE PROCESS DIFFERENCE. The standard deviation of a process difference value that takes into account measurement and non-measurement contributions to the components of the process difference. (10 CFR 74.4, *Definitions*)

STANDARD REFERENCE MATERIAL (SRM). A certified reference material issued by the National Institute of Standards and Technology (NIST) that also meets additional NIST-specified certification criteria. NIST SRMs are issued with Certificates of Analysis or certificates that report the results of their characterizations and provide information regarding the appropriate uses of the materials.

STATISTICAL SAMPLING. A statistically valid technique used to select elements from a population. It includes, but is not limited to, probability sampling, simple random sampling, systematic sampling, stratified sampling, and cluster sampling.

STATUS OF INVENTORY. A reported breakdown (by process, physical, or chemical form) of the physical or book inventory, or a combination thereof, of nuclear materials at a facility at a given time.

STEALTH. Methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear material, where the fact of such attempt is concealed or an attempt is made to conceal it.

STRATEGIC VALUE. The usefulness of a nuclear material to a potential diverter in constructing a weapon.

SUPERVISED LINE. A conductor which, if cut, broken, shorted, or otherwise tampered with, will cause a change in status to be indicated at a monitoring unit.

SURETY. Safety, security, and use control of nuclear explosives.

SURVEILLANCE. The collection of information through devices and/or personal observation to detect and assess unauthorized movements of personnel and nuclear material, tampering with material containment, falsification of information related to location and quantities of nuclear material, and tampering with safeguards devices.

SURVEY. (See SAFEGUARDS AND SECURITY SURVEY, SECURITY SURVEY, and NUCLEAR MATERIALS INSPECTION/SURVEY.)

SYSTEM CONFIGURATION MANAGEMENT. Functions required to inform the host of the site's physical protection system configurations, such as placement of sensors, alarm groups, cameras, and access control devices.

SYSTEM PERFORMANCE TEST. An evaluation of all or selected portions of a safeguards and/or security system as it exists at the time of the test.

T

TACTICAL ENTRY SPECIALIST. A certified Security Police Officer III who is trained in analyzing, selecting, recommending, and employing methods of mechanical and/or explosive techniques for entry into secured spaces.

TAMPER ALARM. An indication that unauthorized access to a security alarm management and control system enclosure or device is being attempted.

TAMPER INDICATING. An item or system element that is either protected by a tamper-indicating device or constructed such that a malevolent act cannot be accomplished without permanently altering the item in a manner that would be obvious during visual inspection.

TAMPER-INDICATING DEVICE (TID). A device that may be used on items such as containers and doors, which because of its uniqueness in design or structure, reveals violations of containment integrity. These devices on doors (and fences) are more generally called security seals.

TAMPER-RESISTANT HARDWARE. Hardware with screws or nut-and-bolt connections that are hidden or cannot be removed with conventional tools.

TAMPER SAFING.

1. The act of applying a tamper-indicating device.
2. The use of a device on a container, vault, or vault-type room in a manner and at a time that ensures a clear indication of any violation of its integrity and the previously made measurements of special nuclear material within it.

TECHNICAL EQUIPMENT INSPECTION (TEI). An inspection conducted at the point of entry by the Defense Threat Reduction Agency in the presence of visiting inspection team members, both upon the team's arrival and departure. It verifies that the equipment used in an inspection has been certified and approved by the United States, does not perform in a manner outside its intended purpose, and complies with safety and underwriting licensing requirements.

TECHNICAL SAFETY REQUIREMENTS (TSRs). Those requirements that define the conditions, the safe boundaries, and the management or administrative controls necessary to ensure the safe operation of a nuclear facility and to reduce the potential risk to the public and facility workers from uncontrolled releases of radioactive materials or from radiation exposures due to inadvertent criticality. TSRs consist of safety limits, operating limits (limiting condition for operation and limiting control setting), surveillance requirements, administrative controls, use and application instructions, and the basis thereof. TSRs were formerly known as "operational safety requirements" for nonreactor nuclear facilities and "technical specifications" for reactor facilities.

TECHNICAL SECURITY. The programs established primarily to protect classified and unclassified controlled information, such as technical surveillance countermeasures, communications security, emission security, and TEMPEST.

TECHNICAL SURVEILLANCE. The covert devices, equipment, techniques, and measures used to obtain unauthorized access to classified and/or unclassified controlled information.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM). The techniques and measures used to detect and nullify the technologies that are intended to obtain unauthorized access to classified and/or unclassified controlled information.

TEMPEST. A short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

TERMINATION BRIEFING. A briefing to inform an individual of his/her continued security responsibilities when his/her DOE access authorization has been or will be terminated.

THEFT. The removal of Government property and/or materials from a DOE or contractor-operated facility without permission or authorization and contrary to law, or the unauthorized removal of special nuclear material. (See also LOSS and DIVERSION.)

THREAT.

1. A person, group, or movement with intentions to use extant or attainable capabilities to undertake malevolent actions against Departmental interests.
2. The capability of an adversary coupled with his/her intentions to undertake any actions detrimental to the success of program activities or operations.
3. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

THREAT ANALYSIS. A process in which information about a threat or potential threat is subjected to systematic and thorough examination in order to identify significant facts and derive conclusions.

THREAT ASSESSMENT. A judgment, based on available intelligence, law enforcement, and open source information, of the actual or potential threat to one or more Departmental facilities/programs.

THREAT INFORMATION. Unevaluated material of every description, at all levels of reliability, and from any source that may contain knowledge or intelligence about a threat.

THROUGHPUT. The measured output of nuclear material, including waste, from a material balance area. (Nuclear Material Control & Accountability)

TOP SECRET (TS). The classification level applied to information, the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security.

TOP SECRET CONTROL OFFICER. An individual who has been designated in writing and has administrative responsibilities for control, handling, accountability, and storage of Top Secret documents generated or received by a Departmental organization.

TRACEABILITY. The property of the result of a measurement or the value of a standard whereby it can be related to stated references, usually national or international standards, through an unbroken chain of comparisons which all have stated uncertainties. (Nuclear Material Control & Accountability)

TRAINING APPROVAL PROGRAM (TAP). A DOE program that formally recognizes S&S training programs and courses conducted by an organization other than the National Training Center that have satisfied established objectives, standards, and criteria for a quality S&S training program or course.

TRANSACTION.

1. Any recorded change affecting an inventory database.
2. Either a physical transfer or a book transfer of nuclear material that is reportable to the Nuclear Materials Management Safeguards System (NMMSS). Each reportable transaction must be recorded using DOE/NRC F 741/741A, *Nuclear Material Transaction Report*, or the electronic equivalent. (See also MATERIALS TRANSACTIONS.) (Nuclear Material Control & Accountability)

TRANSFER.

1. A change in responsibility for securing and or accounting of nuclear material. Transfers can be either physical (e.g., change in physical location of the item) or book (e.g., change in bookkeeping account number). (See also EXTERNAL TRANSFER and INTERNAL TRANSFER.)
2. The passing of custody and control of one government's classified material to another government.

TRANSFER CHECK. The act of verifying the shipping container or item count, verifying the integrity of the tamper-indicating device (including the identification number), and comparing this information with appropriate documentation following the transfer of nuclear material.

TRANSPORTATION SAFEGUARDS SYSTEM. A Departmental system for the safe and secure movement of nuclear devices, nuclear components, special nuclear material, and other cargo deemed appropriate by responsible program elements and approved by the Office of Secure Transportation.

TRANSURANIC WASTE (TRU WASTE). Non-essential or excessed material contaminated with elements that have an atomic number greater than 92, and that are in concentrations greater than 100 nanocurie per gram (nCi/g), or in such other concentrations as the U.S. Nuclear Regulatory Commission may prescribe to protect public health and safety. (42 U.S.C. 2014(ee) [Section 3(ee), as amended, of the Atomic Energy Act of 1954]

TREATY ON OPEN SKIES. A multilateral treaty entered into force in January 2002 which establishes an aerial observation regime using sensor- and camera-equipped aircraft designed to increase transparency and build mutual confidence among participating countries.

TRUE VALUE. A measurement value that would be obtained by a perfect measurement. (Nuclear Material Control & Accountability)

TRUSTED AGENT. A technically knowledgeable individual who acts as a neutral party to assist in planning and conducting a performance test.

TWO-PERSON RULE. Two authorized persons physically located where they have an unobstructed view of each other and/or item(s) and can positively detect unauthorized actions or access to nuclear materials. Other situations, such as use of CRYPTO keying materials, also require application of a similar two-person rule.

U

UNACCEPTABLE RISK. A condition that, if not mitigated, could cause damage to the national security of the United States or impact on Departmental and contractor employees, the public, and/or the environment.

UNAUTHORIZED DISCHARGE. The discharge of a firearm under circumstances other than (1) during firearms training with the firearm properly pointed down range (or toward a target) or (2) the intentional firing at a hostile party when deadly force is authorized by 10 CFR 1047.7.

UNAUTHORIZED DISCLOSURE. A communication or physical transfer of classified or unclassified controlled matter to an unauthorized recipient.

UNCERTAINTY. (See MEASUREMENT UNCERTAINTY.) (Nuclear Material Control & Accountability)

UNCLASSIFIED. The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority.

UNCLASSIFIED CONTROLLED INFORMATION. Unclassified information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552).

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI). Certain unclassified Government information concerning nuclear material, weapons, and components whose dissemination is controlled under 42 U.S.C. 2168 (Section 148, as amended, of the Atomic Energy Act of 1954), DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information.*

UNINTERRUPTIBLE POWER SUPPLY (UPS). An auxiliary power system that supplies battery back-up power when normal power is lost.

UNIRRADIATED MATERIAL. Material that, in its existing form, has not been irradiated in a nuclear reactor or accelerator, or if it has been irradiated, the surface dose does not exceed 10 millirem per hour (mrem/h).

UPGRADE. A determination by an appropriate authority that (1) raises the classification level of information, (2) raises the classification level of matter, or (3) assigns the correct classification level and/or category to matter that was erroneously classified at a lower level (including unclassified) or category.

USE CONTROL. The application of systems, devices, or procedures that allow timely authorized use of a nuclear explosive while precluding or delaying deliberate unauthorized nuclear detonation.

V

VALIDATION.

1. The process used to verify the accuracy of data gathered during an inspection and/or assessment activity.
2. The determination of fitness for purpose of a measurement method applied for routine testing. Such studies produce data on overall performance and on individual influence factors which can be applied to the estimation of uncertainty associated with the results of the method in normal use. Validation studies for analytical measurements typically determine some or all of the following parameters: precision, bias, linearity, detection limit, robustness, and selectivity/specificity. (Nuclear Material Control & Accountability)

VARIANCE.

1. A statistical term relating to a measure of the dispersion of a set of results.
2. An approved condition that technically varies from an S&S directive requirement, but affords equivalent levels of protection without compensatory measures.

VARIANCE PROPAGATION. The determination of the value to be assigned as the uncertainty of a given measured quantity using mathematical formulas for the combination of errors from constituent contributors.

VAULT. A windowless enclosure with walls, floors, roofs and doors designed and constructed to significantly delay penetration from forced entry and equipped with intrusion detection system devices on openings allowing access.

VAULT-TYPE ROOM (VTR). A Department-approved room having combination-locked doors and protection provided by a Department-approved intrusion alarm system activated by any penetration of walls, floors, ceilings, or openings, or by motion within the room.

VERIFICATION MEASUREMENT. A quantitative remeasurement of the amount of nuclear material in an item made to verify the quantity of nuclear material present. Verification measurements, when used to adjust accountability records, must have accuracy and precision comparable to, or better than, the original measurement method.

VIOLATION. Any action or intent that constitutes a violation of U.S. law or Executive order or the implementing directives.

VISITOR. An individual who is not an employee of the site, and who does not work full or part-time at the site. The individual may hold a clearance or access authorization from another agency, but would still be considered a visitor.

VITAL AREA. A type of security area that is located within a protected area and has a separate perimeter and access controls to afford layered protection, including intrusion detection, for vital equipment.

VITAL EQUIPMENT. Equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact to the health and safety of Departmental and contractor employees, the public, or the environment.

VOUCHING. Visually verifying the access authorization of another person for the purpose of piggybacking into a security area. (See also PIGGYBACKING.)

VULNERABILITY. A weakness or system susceptibility that, if exploited, would cause an undesired result or event leading to loss or damage to national security.

1. Major Vulnerability - A vulnerability which, if detected and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.
2. Unspecified Major Vulnerability - A major vulnerability, but specified in no greater detail than the specific security system (or one of its major components) when it occurs.

VULNERABILITY ANALYSIS. A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a S&S system to protect specific targets from specific adversaries and their acts.

VULNERABILITY ANALYSIS REPORT (VAR). A report associated with the S&S management and planning process that describes the methodologies used in vulnerability analyses, sets forth supporting information used, provides the results of vulnerability analyses and risk assessments, and establishes risk ratings.

VULNERABILITY ASSESSMENT (VA). (See VULNERABILITY ANALYSIS.)

W

WAIVER. An approved nonstandard condition that deviates from Departmental directive requirements which, if uncompensated, would create a potential or real vulnerability and, therefore, requires implementation of compensatory measures for the period of the waiver.

WARNING LIMIT. A control limit established for an inventory difference which, when exceeded, requires investigation and appropriate action. NOTE: For processing, production, and fabrication operations, warning limits are established with a 95 percent confidence level.

WASTE. The nuclear material residues that have been determined to be uneconomical to recover. (Nuclear Material Control & Accountability)

WEAPON DATA. Restricted Data or Formerly Restricted Data concerning the design, manufacture, or use (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

WEIGHT PERCENT. A measure of composition. As applied to isotopic composition, it is the fraction obtained by dividing the weight of the isotope of interest in a sample by the weight of the element in the sample and multiplying by 100. It may also be used to specify the fraction of an element in a compound or mixture (e.g., the weight percent of oxygen in UO_3).

WORK FOR OTHERS (WFO). The research, development, testing, manufacturing, or experimentation operations and activities conducted at Departmental facilities for an agency other than DOE.

WORKING PAPERS. Draft document created in the preparation of a final version of a classified document.

WORKING RANGE. The set of values of measurands for which the error of a measuring instrument is intended to lie within specified limits.

WORKING STANDARD. A standard that is used routinely to calibrate or check material measures, measuring instruments, or reference materials and that is traceable to the national measurement base.

X

There are no terms beginning with “X” that require definition.

Y

There are no terms beginning with “Y” that require definition.

Z

ZONE OF OBSERVATION. For perimeter intrusion alarm assessment by closed-circuit television, those parts of the isolation zone and exterior areas of the protected area extending from the nearest points on the ground viewable by the closed-circuit television camera to the similar point on the ground viewable by an adjacent closed-circuit television camera that is pointed in the same direction.

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

SECTION C - ACRONYMS AND ABBREVIATIONS

3-D	Three Dimensional

A

AAAP	Accelerated Access Authorization Program
AC	Advisory Circular
ACL	Adversary Capability List
AIP	Aviation Implementation Plan
AIS	Automated Information System
ANACI	Access National Agency Check and Inquiries
ANSI	American National Standards Institute
ARAPT	Alarm Response and Assessment Performance Test
ARG	Accident Response Group
ASTM	ASTM International (formerly "American Society for Testing Materials")
AWE	Atomic Weapons Establishment

B

BCD	Binary Code Decimal
BD	Blast Deflector
BFA	Blank-Fire Adapter
BMS	Balanced Magnetic Switch
BQC	Basic Qualification Course

C

C	Confidential National Security Information
CAR	Conversion to Carbine
CAS	Central Alarm Station
CBW	Chemical Biological Weapon
CCTV	Closed Circuit Television
CDST	Closed Door Skills Test
CE	Capital Expense
CEO	Chief Executive Officer
C/FGI-MOD	Confidential Foreign Government Information Modified Handling
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
C/FRD or CFRD	Confidential Formerly Restricted Data
CFX	Command Field Exercise
CG	Classification Guide
CI	Counterintelligence
CMPC	Classified Matter Protection and Control
C/NSI	Confidential National Security Information

CNT	Crisis Negotiation Team
CNWDI	Critical Nuclear Weapons Design Information
COEI	Composition of Ending Inventory
COMSEC	Communications Security
CPCI	Central Personnel Clearance Index
CPI	Critical Program Information
CPP	Chamber Porting Procedure
CPR	Cardiopulmonary Resuscitation
CPU	Central Processing Unit
CPX	Command Post Exercise
CQB	Close Quarters Battle
CRD	Contractor Requirements Document
C/RD or CRD	Confidential Restricted Data
CRADA	Cooperative Research and Development Agreement
CRYPTO	Cryptological
CSCS	Contract Security Classification Specification
CTA	Central Training Academy
CTS	COSMIC Top Secret
CTSA	COSMIC Top Secret ATOMAL
CVA	Central Verification Activity
CWACS	Complex-Wide Access Control System

D

DBT	Design Basis Threat
DCID	Director of Central Intelligence Directive
DEAR	Department of Energy Acquisition Regulation
DES	Data Encryption Standard
DGP	Data Gathering Panel
DMC	Dye-Marking Cartridge
DNA	Does Not Apply
DNS	Defense Nuclear Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DSS	Defense Security Service

E

E	Excluded Parent
EA	Exclusion Area
EMT	Emergency Management Team
EOC	Emergency Operations Center
EOCP	Elevated Observation Control Platform
EOD	Explosive Ordnance Disposal

EPP	Executive Protection Program
ESM	Electronic Storage Media
ESS	Engagement Simulation System

F

F	Form
FA	Federal Agent
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FCL	Facility Clearance
FDAR	Facility Data and Approval Record
FGI	Foreign Government Information
FIC	Firearms Instruction Certification
FIPC	Federal Investigations Processing Center
FML	Firearms Modification List
FN	Fabrique Nationale
FOCI	Foreign Ownership, Control, or Influence
FOF	Force on Force
FOIA	Freedom of Information Act
FO	Federal Officer
FOUO	For Official Use Only
FPCO	Focal Point Control Officer
FRAM	Functions, Responsibilities and Authorities Manual
FRD	Formerly Restricted Data
FSO	Facility Security Officer
FY	Fiscal Year

G

GAO	General Accounting Office
GCA	Government Contracting Activity
GO	General Order
GPP	General Plant Project
GRS	General Records Schedule
GSA	General Services Administration
GSC	Government Security Committee

H

H&K	Heckler and Koch
HEPA	High-Efficiency Particulate Air
HQ	Headquarters
HRP	Human Reliability Program
HSPD	Homeland Security Presidential Directive

HVAC	Heating, Ventilating, and Air Conditioning

I

IAA	Interim Access Authorization
IAEA	International Atomic Energy Agency
IC	Instructor Certification
ICT	Inventory Change Type
ID	Inventory Difference
IDS	Intrusion Detection System
IMI	Impact Measurement Index
IND	Improvised Nuclear Device
INFOCIRC	Information Circular
INMTS	International Nuclear Materials Tracking System
ISOO	Information Security Oversight Office
ISSM	Integrated Safeguards and Security Management
ITC	Interagency Training Center

J

JA	Job Analysis
JAIEG	Joint Atomic Information Exchange Group
JCATS	Joint Conflict and Tactical System
JTS	Joint Tactical Simulation
JTX	Joint Training Exercise

K

KMP	Key Management Personnel
KSA	Knowledge, Skill, and Ability

L

LA	Limited Area
LANMAS	Local Area Network Material Accountability System
LAW	Light Anti-tank Weapon
LEA	Law Enforcement Agency
LFSH	Live Fire Shoot House
LICP	Line Item Construction Project
LLEA	Local Law Enforcement Agency
LMG	Light Machine Gun
LRI	Live Round Inhibitor
LRMB	Live Round Magazine Block
LSPT	Limited Scope Performance Test
LSSO	Local Site Specific Only

M

MAA	Material Access Area
MBA	Material Balance Area
MBR	Material Balance Report
MC&A	Material Control and Accountability
MFO	Multiple-Facility Organization
MILES	Multiple Integrated Laser Engagement System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSDS	Material Safety Data Sheet
MT	Material Type

N

NACC	National Agency Check with Credit
NACLC	National Agency Check with Law and Credit
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NC	NATO Confidential
NCA	NATO Confidential ATOMAL
NDA	Nondestructive Assay
NDPC	National Disclosure Policy Committee
NEST	Nuclear Emergency Support Team
NFPA	National Fire Protection Association
NID	National Interest Determination
NIJ	National Institute of Justice
NIOSH	National Institute of Occupational Safety and Health
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NMC&A	Nuclear Material Control and Accountability
NMMSS	Nuclear Materials Management Safeguards System
NMR	Nuclear Materials Representative
NNPI	Naval Nuclear Propulsion Information
NNSA	National Nuclear Security Administration
NOCONTRACT	No Dissemination to Contractors
NOFORN	No Foreign Dissemination
NOL	Normal Operational Losses
NP	Non-possessing
NR	NATO Restricted
NRC	Nuclear Regulatory Commission
NS	NATO Secret
NSA	NATO Secret ATOMAL
NSB	Near-Site Boundary

NSC	National Security Council
NSDD	National Security Decision Directive
NSI	National Security Information
NTC	National Training Center
NVD	Night Vision Device

O

OA	Office of Independent Oversight and Performance Assurance
OADR	Originating Agency's Determination Required
OC	Operations Center
OCI	Office of Counterintelligence
ODNCI	Office of Defense Nuclear Counterintelligence
ODST	Open Doors Skills Test
OE	Operational Expense
OF	Optional Form
OGA	Other Government Agency
OMB	Office of Management and Budget
OPFOR	Opposition Force
OPM	Office of Personnel Management
OPSEC	Operations Security
ORCON	Originator Controlled
OSHA	Occupational Safety and Health Administration
OSO	Office of Special Operations
OST	Office of Secure Transportation
OUO	Official Use Only

P

PA	Protected Area
PB	Paintball
PC	Processing Code
PDF	Portable Document Format
PE	Protection Effectiveness
PED	Portable Electronic Device
PF	Protective Force
PFSC	Protective Force Safety Committee
PIDAS	Perimeter Intrusion Detection and Assessment System
PIN	Personal Identification Number
PIT	Precision Immobilization Technique
PP	Property Protection
PPA	Property Protection Area
PPE	Personal Protective Equipment
PPM	Parts Per Million
PPMA	Parts Per Million Atom
PPMV	Parts Per Million Volume

PO	Post Order
PRFOT	Precision Rifleman Forward Observer Team
PROPIN	Proprietary Information
PSF	Personnel Security File
PSI	Personnel Security Investigation
PT	Performance Test

R

RAR	Risk Analysis Report
RAS	Rail and Alternate Sighting
RD	Restricted Data
REL TO	Authorized for Release to Country
RF	Radio Frequency
RIS	Reporting Identification Symbol
RP	Resource Plan
RPG	Rocket Propelled Grenade
ROE	Rules of Engagement

S

S	Secret National Security Information
SA	Special Agent
SAMACS	Safeguards and Security Alarm Management and Control System
SAMS	Safeguards Management Software
SAP	Special Access Program
SAPF	Special Access Program Facility
SAPOC	Special Access Program Oversight Committee
SAR	Safety Analysis Review
SAS	Secondary Alarm Station
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDZ	Surface Danger Zone
SEC	Securities and Exchange Commission
SECON	Security Condition
SED	Shippers Export Declaration
SF	Standard Form
S/FRD or SFRD	Secret Formerly Restricted Data
SIMEX	Secure Information Management and Exchange Network
SIRP	Security Incident Response Plan
SMG	Submachine Gun
SNM	Special Nuclear Material
SO	Office of Security
SOP	Standard Operating Procedure
SPECAT	Special Category

SPO	Security Police Officer
SPR	Strategic Petroleum Reserve
S/RD or SRD	Secret Restricted Data
SRT	Special Response Team
S&S	Safeguards and Security
SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation – Periodic Reinvestigation
SSIMS	Safeguards and Security Information Management System
SSP	Site Security Plan
SSSP	Site Safeguards and Security Plan
STC	Sound Transmission Class
STU	Secure Telephone Unit
SUCI	Sensitive Use Control Information
S&W	Smith and Wesson

T

TCO	Technology Control Officer
TCP	Technology Control Plan
TE	Tactical Entry
TEC	Total Estimated Cost
TI	Transaction Indicator
TID	Tamper Indicating Device
TJ	Transaction Journal
TPC	Total Project Cost
TS	Top Secret National Security Information
TSCM	Technical Surveillance Countermeasures
TSCMPM	Technical Surveillance Countermeasures Program Manager
TS/FRD or TSFRD	Top Secret Formerly Restricted Data
TSG	Telephone Security Group
TS/RD or TSRD	Top Secret Restricted Data

U

U	Unclassified
UCNI	Unclassified Controlled Nuclear Information
U.K.-C	United Kingdom-Confidential
UL	Underwriters Laboratories
UN	United Nations Organization
UPS	Uninterruptible Power Supply
U.S.C.	United States Code

V

VA	Vulnerability Assessment
VADB	Visitor Access Data Base

VAR	Vulnerability Assessment Report

W

WFO	Work For Others
WMD	Weapons of Mass Destruction
WNINTEL	Warning Notice-Intelligence Sources and Methods

DEPARTMENTAL ELEMENTS TO WHICH
DOE M 470.4-7, *Safeguards and Security Program References*
IS APPLICABLE

Office of the Secretary
Departmental Representatives to the Defense Nuclear Facilities Safety Board
Energy Information Administration
National Nuclear Security Administration
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation/Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration