APPENDIX F

DEFINITIONS

access denial - Refers to methods for preventing any of the following: the knowledge, use, or possession of classified or other sensitive information; the proximity to a nuclear weapon and/or special nuclear material in such a manner as to allow the opportunity to control, divert, steal, tamper with and/or damage the weapon or material; or ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in a Classified Automated Information System.

Atomal - A NATO marking applied to Restricted Data or Formerly Restricted Data provided by the United States to NATO, or to "U.K. Atomic Information" provided by the United Kingdom.

attack - A covert or overt act directed against departmental assets or personnel that, if successful, would result in damage to Departmental property or the environment or injury to Departmental or contractor employees.

automated information system (AIS) -

a. An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. (E.O. 12958)

b. An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material. (NISPOM)

automated information system (AIS) security - Compilation of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy. This includes: all hardware/software functions, characteristics, and features; operational procedures; accountability procedures; access controls at all computer facilities; management constraints; physical protection; control of compromising emanations (TEMPEST); personnel and communications security; and other security disciplines.

book inventory (BI) - The term for the quantity of nuclear material present at a given time as reflected by accounting records.

Category I quantity of SNM Category (sometimes referred to as threshold quantity or trigger quantity or significant quantity of strategic SNM) -

a. U-235 (contained in uranium enriched to twenty-or-more percent in the isotope U-235) alone, or in combination with plutonium and/or uranium-233 when (multiplying the plutonium and/or uranium-233 content by 2.5) the total is 5,000 grams or more. (U)

b. Plutonium and/or uranium-233 when the plutonium and/or uranium-233 content is 2,000 grams or more. (U)

Communications Security (COMSEC) - Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

NOTE: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

COMSEC equipment - Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment is crypto-equipment, crypto ancillary equipment, crypto production equipment, and authentication equipment.

compromise - Disclosure of classified information to an unauthorized person(s). See "Unauthorized Disclosure."

component, nuclear - Weapon components composed of fissionable or fusionable materials that contribute substantially to nuclear energy released during detonation. These include boosting materials but not initiator materials.

convoy - One or more highway vehicles transporting material, equipment, matter and/or personnel organized under the same itinerary for the purpose of safeguarding highway trip(s).

Cosmic - A North Atlantic Treaty Organization marking applied to Top Secret documents prepared by or for circulation within the North Atlantic Treaty Organization.

counterintelligence - Activity intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, and international terrorist activities by or on behalf of foreign powers, organizations, or persons.

Critical Nuclear Weapon Design Information (CNWDI) - CNWDI is NOT a classification; it is an access limiter used primarily within the DoD to control "need-to-know" access for design information on nuclear weapons. (N) is used to indicate CNWDI information. A CNWDI marking should be used on any document going to the DoD that contains information classified by topics marked with an (N). CNWDI is defined as Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermonuclear-type or implosion fission-type bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fuzing or firing systems, limited life components, or total contained quantities of fissionable, fusionable, or high-explosive materials by type. Among these excluded items are the components that service personnel set, maintain, operate, test, or replace.

cryptanalysis - The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.

cryptoprinciple - A deterministic logic by which information may be converted to an intelligible form and reconverted to an intelligible form.

cryptosystem - Associated COMMUNICATION SECURITY items interacting to provide a single means of encryption and decryption.

declassification -

a. The authorized change in the status of information from classified information to unclassified information. (E.O. 12958)

b. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

1. information - A determination by appropriate authority in accordance with approved classification policy that information is no longer classified; or

2. documents or material - A determination by appropriate authority in accordance with approved classification guidance that a classified document or material no longer contains classified information.

3. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation. (NISPOM)

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 covers the meanings of decipher and decode.

Design Basis Threat - A policy statement that describes threats that are postulated for the purpose of establishing requirements for safeguards and security significant programs, systems, components, equipment, information or material.

document - The physical medium on or in which information is recorded or a product or substance which contains or reveals information, regardless of its physical form or characteristics. Documents include written or printed information; removable ADP media (diskettes, tapes, cards, etc.); charts; maps; paintings; drawings; engravings; sketches; photographic prints; exposed or developed film; working notes and papers; reproductions of such things by any means or process; and sound and video recordings by magnetic, optical, or any other electronic means.

downgrading -

a. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level. (E.O. 12958)

b. A determination by appropriate authority that:

1. Information may be handled or discussed at a level lower than the initial classification level, or

2. Documents and/or material may be handled or stored at a level and/or category lower than the initial classification level and/or category.

In either case, the revised classification level shall not be lower than Confidential.

encrypt - To convert plain text into unintelligible form by means of a cryptosystem.

NOTE: The term encrypt covers the meanings of encipher and encode.

escort vehicle (EV) - Normally a van-type vehicle used to carry couriers and equipment for escorting TSS convoys and trains.

Exclusion Area - A type of DOE 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.

exercise - Any scenario that simulates an actual incident requiring a response.

exploitable weakness - A weakness that can be used mainly for the adversary's advantage.

facility - An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

Foreign Government Information - Information that is:

a. 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;

b. Produced by the United States 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

c. Received and treated as "foreign government information" under the terms of a predecessor order to E.O. 12958.

Foreign Intelligence - I

a. Information and product materials resulting from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power, which is significant to the national security, foreign relations, or economic interests of the United States and which is provided by a Government agency that is assigned an intelligence mission (i.e., an intelligence agency);

b. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons (i.e., positive intelligence), but not including counterintelligence (with the exception of information on international terrorist activities; or

c. Information relating to the ability of the United States to protect itself against actual or potential attack by, or other hostile acts of, a foreign power or its agents, or against the activities of foreign intelligence services.

hardening - Measures taken in the design and fabrication of a weapon or its parts to reduce their vulnerability.

heavy shipping container - A thick-walled container (e.g., spent fuel shipping cask) which is used for shipping radioactive materials and which would require the use of high explosives or other such means for breaching in order to effect release and dispersion of its radioactive contents.

highly concentrated easily dispersible form - A form, specific activity, and total activity that can be handled in such a way as to effect a highly significant malevolent dispersal.

highly irradiated material - Material having a radiation level of at least 100 rem/hr at one meter.

highly significant malevolent dispersal - A malevolent dispersal in which greater than Title 10, Code of Federal Regulations, Part 100 criteria or similar levels of respirable, ingestible, or water soluble doses can be received. The profiles (including capabilities) of the perpetrators of such dispersals are defined by the DOE Design Basis Threat Policy or by site or program specific threats developed in Master Safeguards and Security Agreements.

improvised nuclear device (IND) - A device incorporating radioactive materials which is made outside an official U.S. Government or other nuclear-weapon-state program and which has, appears to have, or is claimed to have the capability to produce a nuclear explosion. See "nuclear explosive".

NOTE: The DoD uses the term "Sophisticated Improvised Explosive Device (SIED)" to refer to an IND of comparatively advanced design.

information -

a. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information. (E.O. 12958)

b. Any information or material, regardless of its physical form or characteristics. (NISPOM)

c. Facts, data, or knowledge itself, rather than the medium of its conveyance. (Documents and material are deemed to convey or contain information and are not considered to be information per se.)

Intelligence Community - The aggregate of those organizations and departments of the U.S. Executive Branch that conduct or support various intelligence activities comprising the total national intelligence effort. Pursuant to E.O. 12333, the IC is comprised the following:

a. The Central Intelligence Agency (CIA);

b. The National Security Agency (NSA);

c. The Defense Intelligence Agency (DIA);

d. Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

e. The Bureau of Intelligence and Research of the Department of State;

f. The intelligence elements of the military services (Army, Navy, Air Force, and Marine Corps), the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, and,

g. Staff elements of the Director of Central Intelligence.

inventory difference (ID) - The numerical difference between the nuclear materials book inventory (BI) and the corresponding physical inventory (PI). Expressed mathematically as: BI - PI = ID. The term "total inventory difference" is sometimes used for inventory difference. Formerly called MUF (Material Unaccounted For, an obsolete term).

Low Technology Nuclear Explosive (LTNE) - A simulated nuclear explosive device or design which is made by an official United States Government program for research or training purposes concerning the improvised nuclear device problem. LTNEs do not include U.S. nuclear weapons or nuclear weapon test devices.

malevolent dispersal - A dispersal of radioactive material, resulting from a malevolent act, in which greater than Title 10, Code of Federal Regulations, Part 100 criteria or similar levels of respirable, ingestible, or water soluble doses can be received.

manifest - A list of material being transported from one location to another for a segment of a trip or for the entire trip.

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.

Material Control and Accountability (MC&A) - That part of safeguards that detects or deters theft or diversion of nuclear materials and provides assurance that all nuclear materials are accounted for appropriately.

Military First Destination (MFD) - Designated military locations in the U.S. which receive and accept into the Department of Defence (DoD) stockpile, direct shipments of nuclear ordnance material from DOE/NNSA contractor plants.

national security assets - DOE and DOE 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, sensitive information, critical facilities, and valuable Government property.

nuclear device - A collective term for a nuclear explosive device, including a nuclear weapon, a weapon prototype, or a weapon test device. It may apply to a single stage design, to a primary or secondary, or to a complete staged design. Usually given a designator such as Mandolin, Kingbolt, Tsetse, Skua, Ruth, Rattler, etc.

Nuclear Explosive Like Assembly (NELA) - An assembly that is not a nuclear explosive but 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 represents a weaponized nuclear explosive such as a warhead, bomb, reentry vehicle, or artillery shell. A NELA does not contain an arrangement of high explosives and fissile material capable of producing a nuclear detonation.

nuclear facility - A facility (e.g., Savannah River, Oak Ridge, etc.) for the production, utilization, storage or handling of Special Nuclear Material, including irradiated material that is of national security significance.

nuclear material - Defined in DOE O 474.1A. See Annex E.

Nuclear Materials Courier (NMC) - A TSD employee who is authorized by the AEA to carry firearms and make arrests without warrant during the performance of duties which include the safe, secure movement of nuclear material identified in DOE O 474.1A.

nuclear threat message - A message that threatens (or refers to the committing of) a nuclear-related malevolent act. The threatened 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.

Office of Secure Transport (OST) - The Division of NNSA responsible for management and safe secure movement of Government-owned or consigned matter transported in the TSS.

Official Use Only (OUO) - A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act; or a security classification marking used during the period July 18, 1949, through October 22, 1951.

physical inventory (PI) - 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 or 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.

physical protection (physical security) -

a. The application of physical or technical methods designed to:
   1. Protect personnel;
   2. Prevent or detect unauthorized access to facilities, material, and documents;
   3. To protect against espionage, sabotage, damage, and theft; and
   4. Respond to any such acts should they occur.
b. The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the classified automated data processing system and related equipment.

physical security plan - A facility-specific document (or group of documents) that gives a comprehensive description of the measures employed for the physical protection of property, information, equipment, nuclear materials, and other assets of national interest.

primary - A fission device that is the initial source of nuclear energy, coupled to a secondary stage.

primary plant - The reactor in a naval nuclear propulsion system.

Protective Force or Protective Personnel (Pro Force) - Security officers, security police officers, Transportation Safeguards Division nuclear material couriers and transportation escorts, and other Federal personnel authorized to be armed under section 161k of the Atomic Energy Act and assigned to protective duties involving safeguards and security interests of the DOE.

radiological dispersal device (RDD) - A device which has, appears to have, or is claimed to have, the capability to produce radioactive contamination over an area ***without*** a nuclear explosion.

reporting identification symbol (RIS) - A unique combination of three or four letters which is assigned to each reporting organization by the DOE or the Nuclear Regulatory Commission (NRC) for the purpose of identification in the nuclear materials management data base.

NOTE: The term is also used to refer to the reporting organization to which the RIS is assigned.

Restricted - A former U.S. security classification marking used prior to December 15, 1953; or an active security classification marking used by some foreign governments and international organizations.

risk analysis - : An analysis of safeguards and/or security system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

Safe Secure Railcar (SSR) - A TSSX car modified by the addition of protective and deterrent systems.

Safe Secure Trailer (SST)/Safeguards Transporter (SGT) - A modified standard closed van, dry freight type, semi-trailer which includes necessary cargo tiedown equipment, and temperature monitoring, fire alarm, and access denial systems. Upgraded versions of the SST are referred to as the Safeguards Transporter (SGT).

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.

schedule - Timetable of a TSS trip.

secondary - A nuclear stage physically separate from the primary.

secondary plant - The drive component in a naval nuclear propulsion system

security - An integrated system of activities, systems, programs, facilities, and policies for the protection of RD and other classified information or matter, sensitive information, nuclear materials, nuclear weapons and nuclear weapon components, and/or Departmental and Departmental contractor facilities, property, and equipment.

security communications (SECOM) - A nationwide high frequency radio system which provides a means of communicating with and monitoring the progress of trips moving in the DOE TSS.

security plan - An official document that describes the utilization of resources by a facility to provide protection of the facility, its site(s), and its assets from attack.

security system - An assemblage of people, equipment, hardware and software, structures, plans and procedures, etc., that is used to protect property, information, equipment, nuclear materials, and other assets of national interest and to respond to malevolent acts.

segment - See trip.

shipment - Nuclear explosives, SNM or other matter consigned from one location to another location.

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.

Sigma categories - A DOE term relating to RD and/or FRD concerning the theory, design, manufacture, storage, characteristics, performance, effects, or utilization of nuclear weapons, nuclear weapon components, or nuclear explosive devices or materials.

site -

a. A geographical area where one or more facilities are located.

b. A geographical area consisting of a DOE-controlled land area including DOE owned facilities (e.g., the Oak Ridge Reservation, the Nevada Test Site, the Hanford Site, Idaho National Engineering Laboratory, Rocky Flats Plant, Feed Materials Production Center).

software security measures - Computer programs and/or routines that control, limit, or monitor access, or otherwise protect data or information processed or stored by an AIS.

source document - A classified document (regardless of medium), other than a classification guide, from which information is extracted for inclusion in another document. The classification of the information extracted is determined by the classification markings shown in/on the source document.

source material - Depleted uranium, normal uranium, thorium, or any other nuclear material determined, pursuant to section 61 of the Atomic Energy Act of 1954, as amended, to be source material; or ores containing one or more of the foregoing materials in such concentration as may be determined by regulation.

special nuclear material (SNM) - Plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which, pursuant to the provisions of section 51 of the Atomic Energy Act, as amended, which DOE determines to be special nuclear material; or any material artificially enriched by any of the foregoing, but which does not include source material. See table 1.

spoofing - Deceiving a system so that the system does not perform its intended function (e.g., decoupling of a nuclear detonation by exploding it in a large cavity so that its seismic signal is much smaller than it otherwise would be).

tactical exercise - A planned event, the purpose of which is to evaluate the tactics to be used in response to the event. It may only involve the "Emergency Operations Center" or may involve a force-on-force event. It does not include tests of security hardware unless response tactics are involved.

target - The objective of an attack. Examples of objectives are classified information, nuclear weapons, SNM, facilities, sites, buildings, and security systems.

technical surveillance countermeasures (TSCM) - Techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to classified NSI, RD, FRD, and/or sensitive but unclassified information.

threat -

a. A person, group or movement with intentions to use extant or attainable capabilities to undertake malevolent actions against DOE interests.

b. The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operation.

threat (Foreign Intelligence) - Specific intelligence collection systems or platforms known or suspected beyond reasonable doubt to be operating against DOE and DOE contractor facilities.

Title 10 CFR 100 Criteria - As of this writing, whole body dose of 25 rem at the site boundary, or 300 rem iodine dose to the thyroid. (See most current Title 10 of the Code of Federal Regulations for further details.)

Transportation Safeguards System (TSS) - The program managed and operated by NNSA under the programmatic direction of the Assistant Deputy Administrator for Secure Transportation. The system has administrative and courier personnel, special transport and escort vehicles, and the nationwide high-frequency communications system required to carry out the the safe, secure, domestic transportation of all DOE-owned or controlled nuclear explosives, Category I or II quantities of special nuclear material (excluding naval reactor core shipments), and other cargos deemed appropriate and agreed to by NNSA and respective heads of departmental elements.

Transportation Safeguards System Railcar (TSSX) - The "X" designates to the railroad that it is an individually-owned car and not owned by the railroad.

trip - An assigned movement of shipment(s), or equipment within the TSS. A "segment" is a separate part of a trip.

Unclassified Controlled Nuclear Information (UCNI) - Certain unclassified Government information whose unauthorized dissemination is prohibited under section 148 of the AEA and DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information.*

upgrade - A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided. Such a determination also includes raising the classification level and/or category of information, or documents or material, including correction of classification on such items erroneously issued as unclassified or at too low a classification level or category.

vulnerability (Safeguards and Security context) - The definition below is repeated from the Safeguards and Security Glossary of Terms. For information to be classified, damage to the national security must result from exploiting the information. A vulnerability that could be expected to result in damage to the national security is classified at a level of Confidential. A vulnerability that could be expected to result in serious damage to the national security is classified at a level of Secret. And, a vulnerability that could be expected to result in exceptionally grave damage to the national security is classified at a level of Top Secret. These definitions of Confidential, Secret and Top Secret are included in the Safeguards and Security Glossary of Terms. When the term vulnerability is used in this guide, use of associated information must be tied directly to damage to national security.

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

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.

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 (weapon hardness context) - The susceptibility of a weapon or its components to degradation from adverse environments, particularly the effects of a defensive burst.

weapon data - RD or FRD concerning the design, manufacture, or utilization (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.

THIS PAGE INTENTIONALLY LEFT BLANK