CHAPTER 2

SAFEGUARDS AND SECURITY INFORMATION

A. General Information

This chapter provides guidance for determining if historical records containing DOE/National Nuclear Security Administration (NNSA) NSI pertaining to safeguards and security are to be declassified or have their classification retained beyond 25 years in accordance with the provisions of E.O. 12958. ***Documents containing RD and FRD are not addressed by this document and retain present classification.***

Safeguards and security refers to the physical protection, control, and accountability of nuclear materials and the security of facilities and assets..

The best designed and most conscientiously operated protection system can be defeated by an adversary with sufficient time, information, and resources. Information concerning the protection of department facilities would be of great value to an adversary. The reason for continued protection of safeguards and security information is to deny an adversary information that would aid an adversary in: (1) planning an attack; (2) circumventing, bypassing, or disabling security system components; or (3) defeating protective force efforts to neutralize an attack.

Areas of DOE/NNSA safeguards and security interests include: (1) physical protection of DOE assets; (2) protection of classified information including protection of automated information systems, communications security (COMSEC), and compromise of classified information; (3) vulnerabilities information; (4) control and accountability of nuclear materials; (5) operations security (OPSEC); (6) malevolent dispersal of radioactive material; (7) nuclear threat message; and (8) technical surveillance countermeasures (TSCM).

The term automated information system (AIS) refers to "any equipment or interconnected system or subsystem or equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data, to include computer software, firmware, and hardware." Included in this definition are controllers, microprocessors, word processors, personal computers, automated office support systems (AOSS), memory typewriters, and other stand alone or special computer systems.

COMSEC refers to measures taken to deny unauthorized persons information derived from telecommunications of the United States (U.S.) Government related to national security and to ensure the authenticity of such communications. Communications security results from the application of security measures (including cryptosecurity, transmission security, and emission security) to systems generating, handling, processing, or using national security or national security related information. It also includes the application of physical security measures to communications security information or materials. The classification of all COMSEC equipment and related documentation is determined by the Director, National Security Agency (NSA). Large amounts of classified information are channeled into communication centers and distributed via secure communications systems. COMSEC is vitally important to ensuring the integrity of these communications.

OPSEC is a program designed to deny or mitigate foreign intelligence services or other unauthorized disclosure of such information. Sensitive activities are defined as classified and unclassified facilities, programs, operations, inquiries, investigations, research, exercises, tests, training, and other functions of DOE/NNSA, or its contractors that, if disclosed, could reasonably be expected to adversely affect the national security. Since DOE/NNSA and contractor operations include a variety of sensitive activities, applicable OPSEC measures cover a wide range and tend to be oriented toward specific facilities or operations.

Modern intelligence collection utilizes equipment and devices incorporating state-of-the-art technology to penetrate targeted areas. Such intelligence gathering devices have been discovered in U.S. facilities throughout the world. The detection of a clandestinely installed device is extremely difficult. The purpose of the TSCM program is to detect and deter such intelligence collection.

B. Broad Guidance

Much information concerning safeguards and security, particularly general information regarding this subject area, is unclassified. However, certain information that would be beneficial to a malefactor in targeting, planning, or executing an attack against DOE/NNSA nuclear facilities, nuclear materials, or nuclear weapons, has properly been classified for national security reasons. Some of this classified safeguards and security information has lost its sensitivity with the passage of time and can be declassified.

However in certain cases, information 25 or more years old, concerning a specific vulnerability may still be of use to a malefactor and should retain classification.

Other safeguards and security information requires continued protection because it is indicative of methods, plans, systems, and operations in use today or evolved from earlier ones. Such information provides insight into current measures and warrants continued protection.

Similarly, limited information concerning material accountability has lost its sensitivity with time. Historical information regarding special nuclear material inventory differences (IDs) for a DOE/NNSA site would not be useful today to a malefactor in diverting or stealing SNM, or making a credible nuclear threat, and is, therefore, declassified. Other historical information about material accountability and control, requires continued protection because it reveals information about allocations of SNM to atomic energy defense activities (e.g., nuclear weapons or naval nuclear propulsion). Such information is very likely to be RD or FRD.

OPSEC information would be useful to a malefactor and could lead to a loss of classified information and should, therefore, not be automatically declassified.

A malefactor who wishes to initiate a highly significant dispersal of radioactive material, or to threaten such dispersal, would almost always require multiple acts (e.g., releasing radioactivity by an explosion or other act while almost simultaneously destroying safety and/or containment systems, or the theft of radioactive sources followed by an explosion, or other means of dispersal). Information that can be protected and that would be useful to a malefactor in effecting a highly significant dispersal of radioactive material should remain classified.

Another responsibility of DOE/NNSA is the assessment of, and response to, nuclear threat messages. Threat messages received in the past have demonstrated the need to be prepared for this situation in the future. An important consideration in evaluating a threat message is the message's credibility. Techniques have been developed that attempt to establish this credibility. With regard to nuclear threat messages in general, the fact that a nuclear threat message was received by DOE/NNSA or other cleared agencies is no longer sensitive if revealed in historical documents over 25 years old. However, other information, actual analysis of such threats, and responses to them, warrants exemption from automatic declassification because such information may still be of great value to a malefactor.

Descriptions of TSCM capabilities and specific TSCM threat information are classified to prevent potential adversaries from acquiring information that will assist them in exploiting security program weaknesses or vulnerabilities. Times, locations, plans, and schedules of TSCM activities are classified to prevent adversaries from knowing when to install, remove, or deactivate equipment or transmission paths.

Procedures and standards are protected to restrict information that would aid an adversary's intelligence collection effort or make discovery of those collection efforts more difficult. Investigative methods, equipment, techniques, or indicators of techniques employed in TSCM are based upon information received through sensitive intelligence sources. To protect these sources, the methods, equipment, and techniques or indicators of techniques are classified.

Facts uncovered by TSCM activities are classified to preclude adversaries from knowing that they have been detected and to avoid revealing DOE/NNSA capabilities or providing indicator of techniques.

Historical records, 25 years or older, containing safeguards and security NSI not covered by the specific guidance below are unclassified. However, if there is any question concerning the sensitivity of the information, it should be referred to OCIC for a classification determination. This does not include records containing information classified by statute such as RD and FRD (AEA of 1954, as amended). These records shall be handled, protected, classified, downgraded, and declassified in accordance with the provisions of the AEA and regulations issued under that Act. Reviewers who are not authorized by DOE/NNSA to classify or declassify such documents should not attempt final determinations. Refer to appendix A for information on identifying and handling documents containing potential RD/FRD. In all cases where there is a question concerning the sensitivity of the information, it should be referred to the DOE HQ classification office for a classification determination.

Topics describing information likely to contain or closely related to RD or FRD are marked "(potential for RD/FRD)".

C. Topics

2.0 SAFEGUARDS AND SECURITY INFORMATION

2.1	Threat description or Design Basis Threat (DBT) information in documents dated prior to January 1, 1980	**U**
2.1A	Threat description or Design Basis Threat (DBT) information in documents dated after December 31, 1979 *NOTE:* Declassify when the threat description, DBT, or DBT element has been superseded and no vulnerabilities exist as a result.	**Retain Classification [25X1, 2, 8; EV]**
2.2	Selection criteria for National Security Assets (NSAs)	**U**
2.3	Policy information, such as DOE orders, safeguards and security guides, security and classification policy, requirements, and procedures information	**U**
2.4	Security plan or security system design for a facility or site of national security interest	
2.4.1	Facility and site description not revealing classified information	**U**
2.4.2	System design, operation, site specifics, etc., if the specific plan or system is known to be obsolete and the information is not transferable to another site	**U**
2.4.3	Information about operational security system(s) *NOTE:* Declassify when the system is no longer in use by DOE.	**Retain Classification [25X2; EV]**
2.4.4	Protective personnel requirements, armaments, response times, contingency plans, etc. *NOTE:* Declassify when the site or facility is closed and the information is known to not be transferable to another site.	**Retain Classification [25X2; EV]**
2.5	Automated information systems (AIS)	
2.5.1	Obsolete systems no longer in use by DOE/NNSA	**U**
2.5.2	Security measures *NOTE:* Declassify when the specific system is known to be obsolete or no longer in use by DOE/NNSA.	**Retain Classification [25X2; EV]**
2.5.3	Government or Government supported contractor analyses (including risk analyses) of automated information system security *NOTE:* Declassify when the specific system is known to be obsolete or no longer in use by DOE/NNSA.	**Retain Classification [25X2; EV]**

2.6 Communications security (COMSEC)

DOE
b(2)

DOE
b(2)

DOE
b(2)

2.7 Vulnerabilities information

NOTE: Includes vulnerabilities pertaining to DOE/NNSA sites, facilities, equipment, and operations/procedures.

2.7.1 In documents dated prior to January 1, 1980	**U**
2.7.2 In documents dated after December 31, 1979 *NOTE:* Declassify when the vulnerability no longer exists.	**Retain Classification [25X2, 3, 8; EV]**

2.8 Control and accountability of DOE nuclear materials (SNM and other nuclear materials)

2.8.1 Inventory difference information or information concerning an inability to locate a missing item or quantity of nuclear material *NOTE:* Actual item masses, or information from which actual item masses may be derived, may be RD. Refer to appendix A.	**U (potential for RD/FRD)**

2.8.2 Total site inventory of nuclear materials **U**

NOTE 1: Applies only to inventory of nuclear materials at the total site level that is classified as NSI.

NOTE 2: Inventories at less than a site level, for unclassified programs such as research reactors, critical assemblies, etc. are unclassified.

2.8.2A Inventory difference of source material **U**

2.8.3 Otherwise **Retain Classification (potential for RD/FRD) [25X2; EV]**

NOTE: Declassify when the information would no longer be of benefit to an adversary.

2.9 Operations security (OPSEC)

DOE b(2)

DOE
b(2)

2.10 Malevolent dispersal of radioactive material	
2.10.1 "Highly significant malevolent dispersal" (see Definitions) scenarios and vulnerability analyses	
2.10.1.1 Trivial or generally known methodology	**U**
2.10.1.2 Otherwise *NOTE:* Declassify when the scenario is no longer plausible and no vulnerabilities exist.	**Retain Classification [25X2; EV]**
2.10.2 Results of tests and dispersal experiments that could be applied to malevolent dispersals from a DOE facility *NOTE:* Declassify when the information is no longer of benefit to an adversary.	**Retain Classification [25X2; EV]**

2.10.3 Details of methods that could be applied to initiate a highly significant malevolent dispersal	
2.10.3.1 Generic description of methods that could be used to disperse radioactive material (e.g., fire, explosives)	**U**
2.10.3.2 Otherwise *NOTE:* Declassify when the methods are no longer useful to an adversary.	**Retain Classification [25X2; EV]**
2.10.4 Tests of effects of attacks on heavy shipping containers *NOTE:* Declassify when the information is no longer of benefit to an adversary.	**Retain Classification [25X2; EV]**
2.11 Nuclear threats	
2.11.1 Fact that a nuclear threat message was received by a facility or organization including the text of the message, if no other classified information (RD, FRD, or NSI) is revealed	**U (potential for RD/FRD)**
2.11.1.1 The general contents of a threat message, case histories or general studies without exploitable details	**U**
2.11.1.2 Exploitable details (e.g., detailed scenarios, analyses, responses or individual case histories, including technical and psychological credibility factors, which would assist a malefactor in composing a credible threat message *NOTE:* Declassify when the information is no longer of benefit to a malefactor.	**Retain Classification [25X2; EV]**
2.11.1.3 Analytical techniques used for evaluation of threat message credibility *NOTE:* Declassify when the techniques are no longer used.	**Retain Classification [25X2; EV]**
2.11.2 Questions chosen to extract information from malefactors	
2.11.2.1 A list of questions without elaboration	**U**
2.11.2.2 A list of questions with elaboration *NOTE:* Declassify when the information is no longer of benefit to a malefactor.	**Retain Classification [25X2; EV]**

2.12 Technical surveillance countermeasures (TSCM)

DOE
b(2)

DOE b(2)