CHAPTER 1

BACKGROUND AND BROAD GUIDANCE

A. Background

On March 25, 2003, the President signed E.O. 12958, *Classified National Security Information*. This order requires the automatic declassification on December 31, 2006 of all classified NSI records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under Title 44, United States Code. The order also provides a limited set of exemptions to this general rule, allowing for continued protection of documents falling within specific categories. In succeeding years, a permanent, historical document will be automatically declassified on December 31 of the year that is 25 years from the date of its initial classification unless it has been reviewed and exempted from automatic declassification under this guide.

Since documents containing Restricted Data (RD) or Formerly Restricted Data (FRD) are exempt from the Executive order's provisions, this automatic declassification provision does not apply to many permanent, historical documents. This fact is further emphasized in Section 3155(b) of Public Law 104-106, the National Defense Authorization Act for Fiscal Year 1996, which prohibits the automatic declassification of DOE documents containing RD or FRD. Furthermore, Congress passed additional legislation (Section 3161 of Public Law 105-261, the National Defense Authorization Act for Fiscal Year 1999, and Section 3149 of Public Law 106-65, the National Defense Authorization Act for Fiscal Year 2000) that require specific procedures to ensure that RD and FRD are not inadvertently released during the automatic declassification of records under the Executive order. These procedures are contained in the Special Historical Records Review Plan (Supplement), dated March 1, 2000.

Although E.O. 12958 requires the automatic declassification of NSI records, Public Laws 105-261 and 106-65 (National Defense Authorization Acts for Fiscal Years 1999 and 2000) restrict the declassification of records that have a potential to contain RD and FRD. File series that are not formally certified by the custodial agency as being "highly unlikely to contain RD or FRD," must undergo a page by page review of all documents by reviewers who are trained and certified by DOE to recognize potential RD and FRD before the documents may be declassified and made available to the public. Documents identified by such reviews as having a potential to contain RD or FRD can not be declassified or released and must be referred to DOE for declassification review.

It should also be noted that the requirements for automatic declassification do not apply to classification determinations made under the Atomic Energy Act (AEA) of 1954, as amended. E.O. 12958, section 6.2(a), states:

> "Nothing within this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with provisions of the Atomic Energy Act of 1954, as amended, and the regulations issued under that Act."

Therefore, documents containing Restricted Data and/or Formerly Restricted Data are specifically excluded from the provisions of E.O. 12958.

B. Broad Guidance

Based on the exemption criteria contained in section 3.3 of E.O. 12958, specific areas of DOE NSI have been identified that are unclassified or exempt from automatic declassification.

Information in the following areas is unclassified:

1. Environmental, health, radiation exposure, and safety issues
2. Human radiation experiments

Information in the following areas is exempt from automatic declassification and the E.O. basis for the exemption is shown in square brackets (e.g., [3.3(b)(2)] meaning that the information is exempt based on section 3.3(b), exemption criterion 2):

1. Safeguards and security information related to current security measures at DOE sites or security programs that could:
   a. provide meaningful assistance to a malefactor contemplating theft of special nuclear material (SNM), a nuclear weapon, or weapon component;
   b. provide meaningful assistance to a malefactor contemplating sabotage of DOE nuclear facilities or assets;
   c. meaningfully assist a malefactor in composing a credible nuclear threat message;
   d. be exploited by foreign intelligence service to either enhance its intelligence collection efforts or thwart U.S. counterintelligence efforts; or
   e. provide meaningful assistance in gaining unauthorized access to currently classified information including that in secure communications or in automated information system (AIS) equipment and AISs.

   [3.3(b)(1), (2), (3), (4)and (8)]
2. Transportation safeguards systems used for transporting nuclear weapons, components, and SNM relating to systems still in operation. Examples of these systems include, but are not limited to, details of the safe secure trailers, safe secure railcars, operational procedures, secure communications, threats, and vulnerabilities. [3.3(b)(2), and (8)]
3. Compromise of RD, FRD, or exempt NSI. Such compromise information typically points to where the information can be found in the public domain. [3.3(b)(2)]
4. Unrecovered nuclear weapons and classified components which may provide information that might assist in unauthorized recovery of nuclear weapons or components with resultant compromise of nuclear weapons design information. [3.3(b)(2)]
5. Nuclear Emergency Support Team (NEST) assets, capabilities, equipment, procedures, or operations still being used to:
   a. search for and aid in the recovery of lost nuclear weapons or materials; and
   b. aid the Federal Bureau of Investigation in the event of a crime involving the theft or alleged theft of a nuclear weapon, an improvised nuclear device or a radiological dispersal device, or to commit any other crime involving nuclear weapons, explosives, devices, or nuclear materials.

   Note that for most of our history, NEST stood for Nuclear Emergency Search Team. [3.3(b)(1), (2) and (8)]

6. Information on the vulnerability, hardness and hardening of nuclear weapon delivery vehicles against nuclear weapons effects. [3.3(b)(2)]

7. High-altitude nuclear weapons effects. [3.3(b)(2)]

8. Proliferation of nuclear weapons information, particularly proliferation detection components or systems and methods for spoofing (giving false indications) and tampering, that could assist potential proliferators, hostile nations, and potential adversaries to develop, improve, or use nuclear weapons. [3.3(b)(2)]

9. DOE intelligence information, analyses, or intelligence sources which are still sensitive or which may reveal sensitive information related to the nuclear weapons program. [3.3(b)(1) and (2)]

10. Foreign governments or international organization(s) information which was provided to DOE, or DOE information provided to foreign government(s) or international organization(s), with the understanding that such information be kept in confidence. Such information includes, but is not limited to, information generated pursuant to agreements for cooperation or sensitive high-level energy discussions between DOE (or predecessor agency) officials and foreign government representatives. [3.3(b)(6) and 9]

11. Naval nuclear propulsion information which will assist other nations in the application of nuclear propulsion to naval vessels will provide unauthorized access to information related to the operational characteristics and capabilities of a naval nuclear propulsion plant. [3.3(b)(2), (4), (6), and (9)]

12. Chemical and biological defense information pertaining to C/B agents that would assist a Weapons of Mass Destruction (WMD) proliferator or terrorist organization. [3.3(b)(2)]

13. Critical Energy Infrastructure information that could:

    a. significantly assist a malevolent interest in the sabotage, destruction, or denial of critical energy infrastructure facilities, systems and resources;

    b. reasonably be expected to cause damage to foreign relations or foreign activities of the U.S.; or

    c. compromise intelligence activities, sources, or methods.

    [3.3(b)(8)]

14. Directed Nuclear Energy Systems and Nuclear Directed Energy Systems. [3.3(b)(4)]

15. Space Nuclear Reactor Information [3.3(b)(6) and (9)]

These are the only subject areas that DOE has determined to require protection beyond 25 years. Even though documents containing information within these subject areas are exempt from automatic declassification, the documents are still subject to mandatory and systematic declassification review under E.O. 12958.

When this guide is updated, changes from "Retain Classification" to "Unclassified" will be clearly marked. Any document reviewed using this guide will be prominently marked as such on the front cover, citing use of this guide (DOE CG-HR-3) and the specific topic(s) used as the basis for retaining classification (2.4.3, 7.2, etc.). This will facilitate future reviews of documents after update of this guide. For this reason, wherever possible, topic numbers are preserved in this guide from those in previous editions.

THIS PAGE INTENTIONALLY LEFT BLANK