DEPARTMENT OF ENERGY

Washington, DC 20585

SEP 27 1993

Mr. Steven Aftergood
Senior Research Analyst
Federation of American Scientists
307 Massachusetts Avenue, NE.
Washington, D.C. 20002

Dear Mr. Aftergood:

Enclosed for your information is a copy of the Classification Policy Study that was conducted to determine whether the present Department of Energy (DOE) classification policies and procedures will remain adequate for the coming decade and beyond.

This study represents the first fundamental review of classification policy for nuclear weapons and nuclear weapon-related information since the Atomic Energy Act became law over 45 years ago. It was performed during a time of dramatic world changes, including the breakup of the Soviet Union and the confirmation of the Iraqi nuclear weapons program.

The study was carried out by the Office of Classification, Security Affairs, using a small working group of individuals having broad experience in government and DOE operations. Its conclusions are based on historical research, complemented by the results of over 200 interviews with individuals from DOE and the DOE weapons complex, other Government agencies, Congressional staff, universities, professional societies, industry and industrial associations, and public interest groups. DOE classification policy and the associated classification system to develop and administer procedures for identifying sensitive classified information were the principal focuses of the study. However, the working group found it necessary to broaden the scope somewhat to include policies concerning sensitive, but unclassified, information and some aspects of information security.

With respect to implementation of the study, Recommendation 2 concerning a legislative amendment to permit the communication of limited Restricted Data to other countries under carefully prescribed conditions is already being addressed as a separate issue due to certain urgencies recognized during ongoing arms control negotiations. Recommendation 7 involves a comprehensive review of nuclear weapon-related information with the objective of removing from classification all information that no longer warrants such protection. This recommendation is being implemented in conjunction with the Secretary of Energy's reinventing government initiative on the declassification of information.

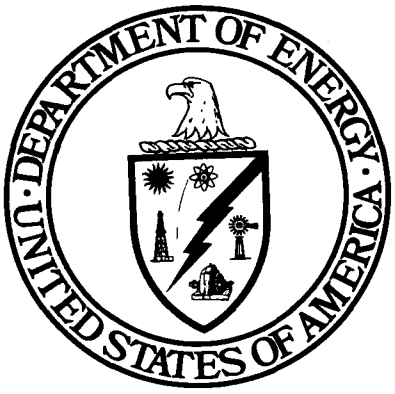
The Department will be reviewing the remaining recommendations of the study for implementation. My thanks for your valuable participation in the interviews by the study team.

Sincerely,

George L. McFadden
Director
Office of Security Affairs

Enclosure

CLASSIFICATION POLICY STUDY



JULY 4, 1992

This study was prepared for the DOE Office of Classification by Meridian Corporation under Contract No. DE-AC01-90DP30414.
This study is under review within the department and no decisions have been made with respect to adoption or implementation of the recommendations herein.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The Restricted Data (RD) system for control of information on nuclear energy, including nuclear weapons and military reactors, was established under the Atomic Energy Act (AEA) in 1946 at a time when the U.S. was seeking to maintain first a monopoly and then a substantial lead over the Soviet Union in nuclear weapons technology. Much has changed since then. Five nations have become acknowledged nuclear powers. India tested a "peaceful nuclear explosive" in 1974. Pakistan has stated that it has a near-term nuclear capability. Israel is thought by many observers to have a substantial nuclear weapon inventory. Other nations such as Iraq have taken major steps to acquire a nuclear capability. Still others have attempted to preserve a future option for nuclear weapons. In addition, the dissolution of the Soviet Union poses new problems concerning ownership and control of tens of thousands of deliverable nuclear weapons and of a very large sophisticated nuclear weapons development capability.

The breakup of the Soviet Union and the aftermath of the Persian Gulf war create significant new requirements and new opportunities for international cooperation on nuclear weapons matters, including nonproliferation, nuclear weapon safety, and arms control. The continuing worldwide diffusion of nuclear weapon-related technology underscores the necessity for such international cooperation. In addition, national security is being increasingly viewed as depending on a healthy economy and a clean environment, and not merely a military capability.

After 45 years under the Atomic Energy Act, and in view of the rapidly changing world situation, it is time for a fundamental review of classification policy for nuclear weapons and nuclear-weapon related information. In March 1990, the Under Secretary of the Department of Energy (DOE) directed a comprehensive classification policy review to determine whether the present DOE Restricted Data (RD) classification policies and procedures will remain adequate and appropriate for the coming decade and beyond. Recent events in the former Soviet Union and Iraq strongly reinforce these concerns. This study is the response to the Under Secretary's direction. Like previous fundamental DOE reevaluations such as those on

security, on waste management and the environment, and on the reconfiguration of the DOE nuclear weapons complex, this review of classification policy is intended to help bring DOE into the 21st century.

This study was carried out by the Office of Classification, Security Affairs, using a small Working Group of individuals having broad experience in government and DOE operations. Its conclusions are based on historical research, complemented by the results of over 200 interviews with people from DOE and the DOE weapon complex, other Government agencies, Congressional staff, universities, professional societies, industry and industrial associations, and public interest groups. DOE classification policy, and the associated classification system to develop and administer procedures for identifying sensitive classified information, are the principal focuses of the Study. However, the Working Group found it necessary to broaden the scope somewhat to include policies concerning sensitive but unclassified information and some aspects of information security.

Present DOE Classification Policy is based principally on the Atomic Energy Act of 1954, as amended, Executive Order 12356, DOE Order 5650.2B, and a hierarchy of Classification Guides. The study examines the extent to which current policy is consistent with the following suggested criteria for nuclear weapons-related information, including isotope separation:

- Classification policy should continue to require protection of information that would significantly help potential adversaries develop an initial nuclear weapons capability or improve existing weapons. It is also necessary to protect information in such areas as possible scenarios for unauthorized use of nuclear weapons, security information for nuclear facilities, and information potentially useful for developing countermeasures to U.S. nuclear weapons.

- The future effectiveness of U.S. classification policy in controlling nuclear weapons-related information requires a fundamental emphasis on international cooperation.

- Nuclear classification policy must take into account its effect on other U.S. national objectives such as environmental cleanup, technology commercialization, and cost reduction.

- Information control and classification policy must take into account the importance of both classified information and sensitive but unclassified information in restraining proliferation.

These guiding principles fully recognize that information control and classification policy cannot prevent, but can only delay nuclear proliferation. The inevitable diffusion of technology worldwide over time means that classification cannot be a permanent solution to proliferation, although it will remain necessary for the foreseeable future as one means of restraining this spread. History shows that proliferation has occurred in many ways, among which are espionage, nation-to-nation technical aid, purchase of technologies or manufactured items, use of unclassified (including declassified) literature, technical education of foreign students, and hiring personnel trained or previously employed in foreign nations in areas relevant to nuclear weapons.

The primary reason that proliferation has not spread more rapidly is that a number of nations with the technical ability to proliferate have made political decisions not to do so. The increasing international level of technological sophistication and the growth of world trade strongly indicate that international cooperation on measures to control nuclear weapons-related technology (including classification policy) is becoming more necessary with time. Communication of RD with foreign governments on a selective basis is necessary not only for international cooperation on nonproliferation but also for arms control and nuclear weapon safety. President Bush has called for discussions with the former Soviet Union concerning cooperation in the area of nuclear weapons safety, including storage, transportation, and destruction; physical security; and command and control. This general approach is being continued with Russia and the other new Republics.

Effective, verified control of nuclear weapons and assurance of their safety will, in the long-term, probably require greatly increased access of foreign inspectors to U.S. facilities. Increased flexibility in classification policy will be needed in future years -- a judgment that is embodied in the recommendations of this study.

Prior to considering specific recommendations for change, the study considered the complete range of both the form and the content of alternative classification systems for protection of information concerning nuclear weapons.

For example, the most radical alternative for both form and content of classification would be to abolish the RD classification system in its entirety and declassify all detailed nuclear weapons design information. This alternative was judged to be infeasible on nonproliferation, public safety, foreign policy, military, and domestic political grounds.

Four other general alternatives for the form or basic structure of a future classification system were considered in some detail:

(1) Retain the current RD system with no structural changes.

(2) Retain the current RD system, but with appropriate legislative or other structural modifications.

(3) Discontinue the current RD system and use the NSI system for all RD information.

(4) Replace the RD system with a new statutory system.

Alternative 1 involves minimum change to a system which has worked for 45 years. However, it does not provide the flexibility needed to adapt the classification system to current circumstances, including the new opportunities and new requirements for international cooperation in areas such as nonproliferation and nuclear weapon safety resulting from the end of the Cold War and concerns about proliferation heightened by Iraq.

Alternative 2, retention of the current RD system but with appropriate structural changes, was judged as providing, on balance, the best compromise between the need for change, and the benefits of maintaining an existing structure.

Alternative 3, replacing the RD system with the NSI system, provides more flexibility than the RD system in dealing with a changing international environment. However, the RD system is better designed than the NSI system for dealing with the long-term protection of scientific and technical information.

Finally, Alternative 4, a new statutory system, was judged to offer little if any advantage over amendments to improve the AEA as described in Alternative 2.

Having selected the general approach of Alternative 2, the following recommendation is made for the foundation structure of classification policy for nuclear weapons-related information during the next decade, and beyond:

- **Recommendation 1: Retain the current Restricted Data system, but with appropriate structural modifications.**

The recommendations provided below for specific modifications to the present RD classification system are intended to make it: more flexible for achieving effective international cooperation in control of nuclear weapons, more credible in identifying what information is truly sensitive, and more generally comparable in operation to the NSI system used for all other classified information. The recommended changes fall into the two categories of structural changes (i.e., amendments to the Atomic Energy Act) and changes in classification policy and operations which can be made largely by the Department of Energy.

The recommended changes that affect the structure of the classification system include:

- **Recommendation 2: Amend the Atomic Energy Act to allow the Secretary of Energy, in coordination with appropriate executive and legislative branch authorities, to approve communication of carefully limited Restricted Data to selected nations for the purposes of more effective cooperation on arms control, nonproliferation, combating nuclear terrorism, and nuclear weapon safety.**

- **Recommendation 3: Amend the Atomic Energy Act to eliminate the Formerly Restricted Data (FRD) category now used to identify military utilization information and transfer such information to NSI.**

- **Recommendation 4: Amend the Atomic Energy Act to allow the Secretary of Energy under carefully prescribed conditions to reclassify specific information in areas of Restricted Data that have previously been declassified.**

- **Recommendation 5: Amend the Atomic Energy Act to eliminate privately generated information from the definition of Restricted Data.**

Recommendations 2 and 3 would permit greater flexibility for international cooperation needed for control of foreign nuclear weapons. Together with Recommendations 4 and 5, they will also make the RD system more effective, more credible, and more comparable to the classification system for other U.S. classified information.

- **Recommendation 6: Amend the Atomic Energy Act to better define the scope and enforceability of Unclassified Controlled Nuclear Information (UCNI).**

Recommendation 6 would help alleviate some of the current problems with sensitive but unclassified information.

In view of the serious reservations many people have concerning amending the AEA, all possible alternative regulatory, administrative, or other non-legislative ways to accomplish these objectives should be carefully evaluated.

Many people interviewed in the course of this study believe that there is now considerable overclassification of information within DOE (although there is no general agreement on what should be downgraded or declassified). Some said that there is now a need for a searching fundamental reevaluation of what information should be protected, and why. Over the past 45 years since the RD system was set up, there have been enormous changes in the world environment; politically, militarily, economically, and technically. It is time for a comprehensive, top-to-bottom review of nuclear weapon-related information to determine what should, and can, be protected. Therefore, in the area of changes to DOE classification policy and operations which do not require legislative or other structural changes, the study makes one very far-reaching recommendation:

- **Recommendation 7: Conduct a comprehensive, fundamental review of all nuclear weapon-related information to determine what should be classified under present conditions, with the objective of removing from classification all information that no longer warrants such protection.**

Implementation of this fundamental recommendation would be a major undertaking and would likely result in major declassifications. It should involve a number of senior people with a wide range of technical expertise and a broad perspective on national security. In addition to people from the nuclear weapons program, the review should involve participation by individuals familiar with worldwide research in relevant areas of technology, with other DOE programs, and with defense, foreign policy, and intelligence. This review would be improved, and it would be more widely accepted, if some of the

participants are "outsiders," i.e., not currently associated with DOE and the government, but from industry and universities.

The review is likely to result in significant declassifications and downgradings. There may also be some limited reclassifications (if Recommendation 4 is implemented) or upgradings. The study suggests that the review is likely to find that declassification in several areas would have sufficient programmatic and other benefits to outweigh any current risks. Illustrative examples include declassification of:

- All wastes not identifiable with specific weapons or tests.
- Fact of all nuclear tests and their yields.
- Inventories and production rates of nuclear materials and nuclear weapons.

New classification policy based on the recommended fundamental review should be implemented in the hierarchy of classification guides. A new Classification Policy Guide describing overall general classification policy in narrative form should be prepared taking into consideration the current standards and criteria for continued classification. Program Guides and Local Guides for all classified DOE programs should then be updated. In the future, such major fundamental reviews should be scheduled for reasonable intervals, such as every 6 years, or when required by major policy changes.

In addition to the formal recommendations for changes in DOE's classification system, the study also makes a number of suggestions or observations. These differ from the recommendations in that they are more narrowly focused, or involve areas that do not require near-term action or are only associated with classification, such as information security.

The study suggests that, in view of the close interaction between classification and security, current information security policy should be examined for security changes needed in order to fully implement the

recommended changes in classification policy. For example, greater use of the level of Top Secret, as suggested by the study, would be impractical without appropriate modifications in document control. These and other suggested changes would make the RD system and the NSI system more comparable, reflecting the principle that the requirements for access to a specific piece of classified information should be uniform throughout the government.

The study further observes that a formal process is needed to estimate the direct and indirect costs of classification as a part of the process of deciding whether proposed declassifications present undue risk.

The primary goal of the recommended structural (e.g., legislative) changes to the RD classification system is to make it more flexible and effective in responding to a rapidly changing world and domestic environment, including facilitating broad national and international goals in nonproliferation, nuclear safety, and arms control. The primary goals of the recommended changes in RD classification policy are to increase the efficiency and credibility of the classification system, and to minimize its negative impact on other domestic national goals such as environmental cleanup and technology commercialization.

Above all, the changes recommended by the study are intended to help the DOE classification system meet the future demands of a changing world.

2. INTRODUCTION

Nuclear weapons have for more than forty years provided the cornerstone for U.S. national security and set limits on the behavior of the great powers. From their inception, nuclear weapons have been justifiably viewed as vastly different from other weaponry, so different that their use in war would constitute passage through a firebreak into warfare of inconceivable horror.

Recognizing this, and wishing to retain the monopoly the U.S. held in nuclear technology, the Congress established in the Atomic Energy Act of 1946 the Atomic Energy Commission (AEC) to manage military and civil nuclear technology and defined the Restricted Data (RD) classification system to place special controls on technical information pertaining to all applications of nuclear energy. The objective was to prevent or delay the spread of nuclear weapons-related technology to other nations. Amendments to the Act in 1954 made certain areas of nuclear information more accessible to the U.S. military, to U.S. industry, to foreign allies, and to the world.. The amendments also specified criteria and procedures for removal of information from the RD category, i.e., declassification. While a good deal of declassification has since taken place, the RD system has remained essentially the same as it was in 1954.

Much has changed since the 1950s. Five nations are acknowledged nuclear weapons states. Israel is thought by many observers to have a substantial nuclear weapon capability. India tested a "peaceful nuclear explosive" in 1974. Pakistan claims to have a near-term nuclear capability. Other nations such as Iraq have made major efforts to become nuclear powers. The breakup of the Soviet Union almost instantly created several new states with nuclear weapons within their borders. Along with this, the discovery of the scope of the Iraqi nuclear weapons program placed new emphasis on international cooperation on control of nuclear weapons, including arms control and nonproliferation. The role of nuclear weapons in military strategy is being reexamined. Further, the economic dimension of national security is now being viewed as comparable to that of national defense.

In March, 1990, DOE's Under Secretary directed that the Department of Energy undertake "... a comprehensive classification policy study to determine whether continuation of the present Department of Energy (DOE) classification policies and procedures will remain adequate and appropriate for the coming decade and beyond." (See Classification Policy Study Charter, Appendix A.) This report has been prepared in response to that directive. It provides the first comprehensive review of overall DOE classification policy since the 1954 revision of the Atomic Energy Act.

The Under Secretary's memorandum provided the following perspective:

> "The world situation is vastly different than the one that existed in 1947 when the Atomic Energy Act became effective. The U.S. nuclear monopoly has long since ended. There has been a significant impact on our economic posture as a result of increased world-wide competitiveness. The cold war seems to be on the verge of ending. Arms control negotiations have brought an Intermediate Nuclear Forces (INF) Agreement with the prospect of others to follow. The Department, in turn, is continuing to face new challenges and goals: an initiative for effectively commercializing technology developed in DP's laboratories to enhance U.S. economic competitiveness, a comprehensive environmental restoration program, a major plan for modernization of the nuclear weapons complex, etc. All these and other factors argue for a fresh look at our DOE classification program to ensure that our policies and procedures are in step with the new national and international environment and the role that the Department will play."

Subsequent events, particularly in the former Soviet Union and Iraq, strongly reinforce these concerns.

Accordingly, this study has the following principal objectives:

- To examine the underlying philosophy of the current classification system and consider alternatives in light of current and anticipated future needs.

- To present a possible "action plan" consisting of suggested structural changes (legislative, regulatory, or administrative) and revisions to classification policy and operations.

The study focuses primarily on the Restricted Data classification system, with the principal aim of assessing how well the current DOE classification system meets modern requirements for national security.

This study does not attempt to determine the level of classification appropriate for specific items of information. It does, however, suggest changes in classification in several broad areas that would better reflect current judgments of sensitivity.

While the principal focus here is on RD, the study also deals with National Security Information (NSI), classified under Executive Order. DOE uses and generates NSI, as do most Federal agencies, but the emphasis here is on the relationships between RD and NSI, and not on the detailed workings of the NSI system.

Classification is concerned with what information should be protected, information security with measures to protect classified information. In DOE, security policy is distinct from classification policy, and a review of security policy is not within the scope of this study. Nevertheless, information security and classification are often closely intertwined, and security implications of several of the major recommendations and observations are addressed.

Similarly, the study goes beyond the strict definition of classification policy to consider policies for the control of sensitive but unclassified

information. Information of this type is assuming greater importance in DOE relations with the public, industry, and academia. It remains an integral part of the effort to protect information which could contribute to proliferation.

Section 3 presents the Study Methodology. The study is based primarily on information and opinion obtained from a large number of people and institutions from DOE, other parts of the government, and outside the government.

Section 4 provides background on the history and structure of national security classification in the United States, a brief history of proliferation, and a discussion of the likely future role of classification.

Section 5 presents study findings, issues raised, a discussion of options, some observations or suggestions, and where appropriate, specific recommendations. Three general areas are addressed:

- Alternative classification systems.
- Legislative or other structural changes to the current Restricted Data classification system.
- Changes in DOE classification policy and operations.

The last section, Section 6, provides general conclusions and a summary list of observations and recommendations.

Appendices include the study charter and other supporting information.

3. STUDY METHODOLOGY

This Classification Policy Study was done under the direction of the Office of Classification (OC) by a Working Group of four individuals with extensive experience in national and international security, DOE policy and operations and the nuclear weapons program in particular. The Working Group members were: Dr. Ray Pollock (Director), Dr. William Grayson, Mr. John Griffin, and Dr. Robert Post.

The Working Group examined relevant statutes, Executive Orders, DOE orders and regulations, reports, historical files of the Office of Classification, and other records. In the early stages, questionnaires and draft issue papers were distributed to a selection of knowledgeable people. However, the primary method used to identify issues and possible solutions was to obtain information, judgments, and opinions from a very wide range of people. More than 200 people were consulted from inside the DOE nuclear weapons complex and elsewhere in DOE*, other government agencies, congressional staff, universities and professional societies, industry and industrial associations, and several interest groups that have indicated concerns in this area (see Table 1 and Appendix C).

The Working Group contacted people by letter or telephone and then, in most cases, followed up with personal or group interviews. To thoroughly cover the central issues and interview a wide range of the people most directly involved, the Working Group went to Albuquerque, Los Alamos, Livermore, and Oak Ridge to interview individuals from Sandia National Laboratories, DOE's Albuquerque Field Office, the seven integrated contractors for nuclear weapons production, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and (at Oak Ridge) Y-12, K-25, Oak Ridge National Laboratory, and DOE's Oak Ridge Field Office.

---

*The Office of the Deputy Assistant Secretary for Naval Reactors declined to participate. Accordingly, the views of the Naval Reactors Program were not included in this study.

TABLE 1
INDIVIDUALS AND INSTITUTIONS CONSULTED

- DOE PROGRAM OFFICIALS
- DOE FIELD OFFICES
- DOE PLANT AND LABORATORY OFFICIALS
- DEFENSE NUCLEAR FACILITIES SAFETY BOARD
- ADVISORY COMMITTEE ON NUCLEAR FACILITY SAFETY
- CURRENT AND FORMER GOVERNMENT OFFICIALS FROM THE DEPARTMENTS OF DEFENSE, STATE, AND JUSTICE, THE ARMS CONTROL AND DISARMAMENT AGENCY (ACDA), THE NUCLEAR REGULATORY COMMISSION (NRC), AND THE CENTRAL INTELLIGENCE AGENCY (CIA)
- INFORMATION SECURITY OVERSIGHT OFFICE (ISOO)
- CONGRESSIONAL STAFF -- House and Senate Armed Services (HASC, SASC), Senate Governmental Affairs (SGA), and House Energy and Commerce (HE&C) Committees
- INDUSTRY -- 30 Trade Associations
- PROFESSIONAL SOCIETIES -- American Association for the Advancement of Science (AAAS), American Chemical Society (ACS), American Institute of Aeronautics and Astronautics (AIAA), American Nuclear Society (ANS), American Physical Society (APS), American Society of Mechanical Engineers (ASME), Institute of Electrical and Electronic Engineers (IEEE)
- NATIONAL ACADEMIES OF SCIENCE AND ENGINEERING
- INTEREST GROUPS -- Natural Resources Defense Council (NRDC), Federation of American Scientists (FAS), Nuclear Control Institute (NCI), Union of Concerned Scientists (UCS), American Civil Liberties Union (ACLU), Environmental Defense Fund (EDF), Carnegie Institution

The people interviewed included current and former policy-level U.S. Government officials, managers, scientists, engineers, experts in non-proliferation and arms control, intelligence experts, specialists in classification and security, legal experts, environmentalists, nuclear weapon designers, and many others. A list of standard questions was developed and used, along with open discussion.

As might be expected, the range of views was extremely broad. Some completely supported the current DOE RD classification scheme. Others advocated tightening up the system to better protect against potential adversaries or proliferators. Still others thought the system should be abandoned as an ineffective anachronism.

The Working Group carefully considered all of the views expressed. It then organized this information and evaluated it to identify common themes and issues. Possible solutions to those issues were identified, taking into account many suggestions from the interviews. Early drafts of this study were widely distributed to DOE Headquarters and Field Offices for review and comments.

The next section, Section 4, presents some useful background information about the current DOE classification system, proliferation over the past four decades, and the expected future role of classification. Study findings and recommendations are given in Section 5.

4. BACKGROUND

4.1 THE CURRENT DOE CLASSIFICATION SYSTEM

4.1.1 Classification in the National Interest

Secrecy, or measures to control access to information, is a well-established right and duty of governments. Classification is a systematic approach to identifying that information which is to be kept secret. The present classification system is of fairly recent origin; its history is recounted in the following subsection of this report and in greater detail in Appendix B. Information security is concerned with how the confidentiality instituted by the classification system is protected. One important aspect is personnel security, including clearance of individuals to certify that their character, associations, and loyalties are such that their access to classified information will not be inimical to the common defense and security. Another aspect is a narrower determination by each program of the specific classified subject areas to which an individual needs access in order to do a particular job, or "need-to-know."

Classification under the Restricted Data (RD) classification system, first established by Congress in the Atomic Energy Act of 1946, is the major focus of this study. In crafting the Atomic Energy Act, Congress intended to preserve the U.S. nuclear monopoly, and to ensure that control of nuclear weapons remained firmly in civilian hands. Clearly, the major goal at that time was to keep nuclear technology from the Soviets.

Throughout the 1950s and 1960s the RD system became institutionalized and generally functioned smoothly. Civilian nuclear power was declassified in the 1950s to facilitate a civil nuclear power program. Attention was focused on weapons technology, which was developing rapidly in response to the Soviet threat. For the classification system, the goal was to safeguard this rapidly emerging technology. While most nuclear reactor technology was declassified, there was little incentive to declassify nuclear weapons or military reactor information except in cases where classification imposed unreasonable burdens

on AEC operations. The technology of nuclear weapons appeared to be good for little else other than military applications.

By 1970, the situation had begun to change. The era of high turnover in the nuclear weapon stockpile had ended. Technical advances in other fields, such as lasers and computers, provided opportunities to apply knowledge and skills developed in the weapons program toward other goals. Interest and expertise in areas that had once been the exclusive province of the weapon laboratories grew in industry and universities, worldwide. Accordingly, the task for classification authorities became more complex.

In the 1990s, many now view international competition in a wide variety of areas of trade as the most serious challenge to U.S. national security in the long term. If technologies with commercial potential exist in classified programs, and there are strong incentives to market them, there will be mounting pressure to declassify them. In addition, environmental cleanup of DOE facilities and requirements for full disclosure concerning shipment of hazardous wastes are increasing the pressure to declassify the composition of DOE wastes, which could reveal specific compositions of materials used in U.S. nuclear weapons. Finally, the international diffusion of basic technology over the past four decades makes today's environment fundamentally different from that of 1945 from the standpoint of nuclear weapons-related classification.

The military threat has changed dramatically over the last few years, with the end of the Cold War and the breakup of the Soviet Union. Nevertheless, reduction in the threat of superpower involvement has allowed ancient rivalries and animosities to resurface, and the threat of conflicts in Europe and Asia to reappear. And, as the Persian Gulf war made very clear, Third-World powers in critical areas of the world can wreak havoc. International inspections found that Iraq was considerably closer to a nuclear weapon capability than was generally believed. This grim finding places an even greater premium on measures to discourage proliferation of nuclear weapons.

The RD classification system was originally established to preserve the U.S. nuclear monopoly. While international controls on exports of critical materials and technology now provide perhaps the most important technical barriers to proliferation, proliferation concerns will always weigh heavily in any question of declassification of nuclear weapons-related information.

Much of the general conceptual and basic information required to develop primitive nuclear weapons (and even thermonuclear weapons) has been available in unclassified form for some time. However, nonproliferation efforts at the technical end of the spectrum continue to serve a very important purpose by maximizing the cost and technical difficulty, and thereby the uncertainty of making a workable nuclear weapon. No proliferator is assured of initial success, since this depends on knowledgeable individuals with specific skills, numerous bits of practical information, and perhaps even an element of luck.

Given that no technology can be protected indefinitely, a fundamental goal of classification policy, worldwide, has been to buy time for possible political solutions to the threat of nuclear weapons by avoiding the release of any information which could significantly reduce the time and effort of a non-nuclear nation in developing the capability to construct a nuclear explosive device. The central task is then to identify this non-public information and balance its practical value for would-be proliferators against the burden that continued classification places on the efficient operation of the U.S. defense community and other U.S. interests, including economic well-being and foreign relations. Similar concerns in other countries should help in the development of essentially similar shared policies on classification and on export control.

As a result of the current international situation, there are new needs, as well as new opportunities, for increased international cooperation on arms control, nonproliferation, and nuclear safety. This is likely to result in an increased need to share some now-classified information, and hence for a reappraisal of current classification and security policies to ensure that they are consistent with these broader needs. For example, verification procedures for future arms control treaties are likely to include highly

intrusive on-site inspections which could reveal some information that is now Restricted Data. While this RD would be of little value to advanced nuclear weapons states, neither the U.S. nor the other nuclear weapon states would want to make it available to potential proliferators. Overall policy for control of sensitive nuclear weapon-related information would have to be changed in order to provide such flexibility.

Finally, classification is expensive. It imposes budgetary, administrative, and programmatic costs on DOE operations, and inevitably restricts commercial use of technologies that could improve economic competitiveness. With DOE in the process of reshaping and rebuilding ("reconfiguring," even partially "privatizing") the weapon complex in an era of shrinking defense budgets, measures that could reduce the cost of operations cannot be ignored. Neither can opportunities for cooperative development and commercialization of competitive technologies. The problem for classification is to provide a system for protection of nuclear weapons-related and military reactor information that is effective in meeting the needs of national security, both economic and military, without undue effects on other national interests.

These issues frame classification policy, and this study.

4.1.2 History and Structure of the DOE Classification System

Most information whose unauthorized disclosure would damage national security is now classified under Executive Order 12356 as "National Security Information" or NSI, and will be described later. The separate system to set and administer policy for the nuclear-related classified information called "Restricted Data" will be described first.

Atomic Energy Act - Restricted Data

With the approval by President Roosevelt in October 1939 of uranium research (based in part on Albert Einstein's letter alerting him to the possibility of building "extremely powerful bombs" using uranium), the first of many

decisions had been made that would lead to the Manhattan Project and the successful U.S. effort to build an atomic bomb.

The Manhattan Project was carried out under a mantle of military security where essentially all information was classified. The degree of secrecy and compartmentalization of information was an irritant to many of those working on the Manhattan Project, who considered it a major impediment to success (though perhaps necessary under the circumstances). Following the two atomic bomb attacks on Hiroshima and Nagasaki, and a few days before the surrender of Japan on August 14, 1945, the United States released a fairly detailed account of the Manhattan Project, the "Smyth Report": H.D. Smyth, "A General Account of the Development of Methods of Using Atomic Energy for Military Purposes under the Auspices of the United States Government, 1940-45." While there was some adverse reaction to releasing so much sensitive information, pressure continued to build inside the Manhattan Project for declassification of various aspects of the project.

Early in November 1945, in response to an avalanche of requests from scientists and contractors to declassify their wartime research and development in atomic energy, Dr. Richard Tolman, President of the California Institute of Technology, was designated to head a committee of distinguished senior scientists to develop a declassification policy for the great volume of classified information that had been generated during the Manhattan Project. The Tolman Committee subsequently developed the first declassification policy, which was published in March 1946 as the "Declassification Guide for Responsible Reviewers."

It is worth noting that when the first declassification guide was published there was no Atomic Energy Act, no Atomic Energy Commission, and no category of classified information known as "Restricted Data". However, the work of the Tolman Committee and the classification system of the U.S. Army's Manhattan Project formed the basis for the classification program of the Atomic Energy Commission when it came into existence in January 1947.

The legislative battle to pass the Atomic Energy Act of 1946 stretched over a period from October 1945 until July 1946. While a number of contentious issues were debated, the overriding concern was civilian versus military control of atomic energy. There was also much controversy over Section 10 which at one point was titled "Dissemination of Information" but was later changed to "Control of Information." Section 10 contained the definition of Restricted Data (RD) as:

> ...all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security.

Later, in 1954, a major revision of the Atomic Energy Act made several significant changes related to the handling and dissemination of RD. Those changes that affected classification were consistent with other changes in the 1954 Act that were designed to make certain atomic energy information more accessible to the U.S. military, to U.S. industry, to U.S. allies, and to the rest of the world. This objective was also reflected in President Eisenhower's Atoms for Peace initiatives which were included in his 1953 speech to the United Nations. These initiatives were directed toward developing the industrial applications of atomic energy. As a result, the 1954 Act contained provisions that related to the classification, declassification, and dissemination of RD that were not contained in the 1946 Act. (See Appendix D for details on these provisions, which are included in section 142 of the Act.)

The provisions of the 1954 Act that concern classification of RD information are essentially unchanged today, and represent the legal foundation and basic structure of the current DOE RD classification system.

Over the years much information which was once RD has been declassified, largely to facilitate commercial applications. Complete program areas such as

civil power reactors and nuclear fuel reprocessing have been removed from the RD category through declassification. Whereas essentially all atomic energy information was classified in the early days, there is now only a relatively small number of remaining areas of national defense-related nuclear information which contain RD:

- Nuclear weapon design
- Nuclear material and nuclear weapon production
- Inertial confinement fusion
- Military reactors
- Isotope separation
- Directed nuclear energy systems

In addition to its statutory basis, there are several unique features of RD that distinguish it from other classified information. RD is generally technical, rather than policy or operational, information. It does not take a specific act by an authorized person to classify RD. Information that falls within the definition of RD is classified when it is originated; i.e., it is "born classified." National Security Information (NSI), on the other hand, is essentially "born unclassified" (except for foreign government information and certain intelligence information). An authorized person must specifically determine that such information is classified. RD information can only be declassified if it meets the criterion contained in the Act (i.e., that it may be published without undue risk to national security) by a person specifically delegated this function by the Secretary of Energy (now the Director of the Office of Security Affairs).

Another unique feature of RD is that it applies not only to information owned or controlled by the government but to all information falling within the RD definition, including that originated in the private sector, hence the term "private Restricted Data." While this provision of the Act has been subject to controversy, it has been successfully applied in a number of cases.

The Act also provides for removing information primarily related to military utilization from RD and putting it under joint control of the DOD and DOE, to

be treated as NSI domestically but remain subject to a formal Agreement for Cooperation for international dissemination. This category of information is known as "Formerly Restricted Data" (FRD). In addition, foreign intelligence information of an RD character may be transclassified to NSI by the joint action of the Director of Central Intelligence and DOE.

The RD classification system differs in a number of fundamental ways from NSI which is classified under Executive Order 12356. NSI is discussed in more detail below.

National Security Information (NSI)

All U.S. classified information other than nuclear-related information (RD or FRD) is currently classified under Executive Order 12356 as "National Security Information" (NSI).

While the classification of military information dates back as far as the earliest days of the United States, the origins of the present national security classification system can be traced to just prior to World War I. However, the first use of an Executive Order for security classification took place when President Roosevelt issued Executive Order 8381 in March 1940, titled "Defining Certain Vital Military and Naval Installations and Equipment." As authority, he cited the Act of January 12, 1938 (Public Law 418, 75th Cong., 52 Stat. 3), which stated:

> Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installation or equipment without first obtaining permission of the commanding officer.

Violation of the law was subject to criminal penalty, a $1,000 fine and/or imprisonment of up to 1 year.

This order was general in nature and relatively brief (about 1 page). The present Executive Order 12356 consists of a very detailed 12-page compilation of policies and procedures. For example, Executive Order 12356 includes the following:

- Definition of Top Secret, Secret, and Confidential as that information whose unauthorized disclosure reasonably could be expected (respectively) to cause "exceptionally grave damage," "serious damage," or "damage," to national security.

- Identification of ten categories of information to be considered for classification.

- Limitations on classification (e.g., basic research not clearly related to national security may not be classified, and classification may not be used to conceal administrative error or violations).

- Procedures for declassification, downgrading, and safeguarding information.

(See Appendix B.2 for a detailed discussion and comparison of the various features of Executive Orders for the classification of National Security Information.)

Over the past 50 years that Executive Orders have been used to promulgate national security classification policy, a much more formal and organized system has evolved. While this system is subject to change with each new Administration, this has not always happened. Where a new Executive Order has been issued by a new Administration, the changes have usually reflected more a change in tone than in substance. However, the fact that a new Executive Order can be issued that changes classification policy without congressional involvement has caused some congressional and other support for a statutorily-based classification system for all information classified for

national security, similar to that incorporated in the Atomic Energy Act for Restricted Data.

The major differences between NSI and RD are summarized in Table B-2, Appendix B.

4.1.3 Operation of the DOE Classification System

The DOE classification system to develop and administer classification policy is based on the Atomic Energy Act (see Appendix D) for RD and on Executive Order 12356 (see Appendix E) for NSI. The system includes both government and contractor classification elements under the direction of the Secretary, the Under Secretary, and the Office of Security Affairs, with day-to-day operational responsibility assigned to the Director of the Office of Classification (See Appendix B.3 for more detailed description of the DOE classification system.)

The DOE classification system is highly centralized. Policy, procedures, orders, and guidance originate in the Office of Classification (OC) and are disseminated to DOE Program Offices, Field Offices, and contractor organizations. The DOE classification program, although closely related to the DOE security program, is clearly separate and distinct. This distinction has existed from the earliest days of the Atomic Energy Commission, based on the principle that classification and security should be treated separately in order to maintain the integrity of each program.

The Office of Classification fulfills its responsibilities by carrying out the following functions:

- Develop, implement, and interpret DOE classification and declassification policy, guidance, rules, regulations, and procedures.

- Initiate and recommend to the Director of the Office of Security Affairs all actions for removing information from the RD and FRD categories.

- Perform interagency and international classification coordination and cooperation.

- Manage programs for classification and declassification review of documents and other materials.

- Develop classification and declassification education and training programs, and administer such programs for DOE headquarters personnel and, as required, for field personnel.

- Appraise the effectiveness of the classification function of Departmental Elements and contractor organizations.

- Develop policies and procedures for the identification and control of Unclassified Controlled Nuclear Information (UCNI).

DOE classification policy is implemented through a hierarchy of classification guides. In principle, the Policy Guide provides overall classification policy that serves as the basis for the Program Classification Guides. These give the classification levels assigned to information within specific programs. Based on these program guides, Local Guides are developed by the DOE Field Offices and contractor organizations to provide detailed, site-specific classification guidance. There are currently over 800 classification guides covering a wide spectrum of DOE programs.

The Office of Classification is also responsible for developing and issuing general and topical guidelines for the identification and control of Unclassified Controlled Nuclear Information (UCNI), as defined in sec. 148 of the AEA. The guidelines cover DOE production and utilization facilities, safeguards and security information, and certain declassified nuclear weapons information.

The authority to declassify RD and FRD is currently delegated by the Secretary of Energy to the Director of the Office of Security Affairs. In the case of RD information relating to nuclear weapons, the DOE normally informally coordinates declassification actions with the DOD and, as appropriate, with the Department of State and CIA. FRD can only be declassified by joint action of the DOE and the DOD.

In order for information to be classified as NSI it must concern at least one of the classifiable areas specified in Executive Order 12356 and the unauthorized disclosure of the information must reasonably be expected to cause damage to the national security. NSI may only be declassified in DOE by the original classifier of such information or by the Director of the Office of Classification.

RD, FRD, and NSI may be transmitted only to persons having appropriate security clearance and a valid "need-to-know" in their work. RD or FRD may be transmitted to a foreign nation or a regional defense organization only if there is a formal Agreement for Cooperation between the receiving party and the U.S., entered into in accordance with the provisions of section 123 of the Atomic Energy Act of 1954, as amended, and implementing statutory determinations under sections 91c, 144b and 144c, as appropriate (see Appendix D).

Need-to-know is administered by each classified program granting individual access to information as needed. This information has been grouped into compartments, generally along program and topical lines. DOE uses a Sigma-numbering system to identify several distinct compartments of nuclear weapon data classified RD or FRD. For example, the Sigma 1 category covers information concerning the theory of operation or complete design of thermonuclear weapons or their unique components. DOD uses the label "Critical Nuclear Weapon Design Information (CNWDI)" as an access limiter to control access to nuclear weapon design information. (CNWDI and Sigma categories overlap. They are discussed in more detail in Appendix B.)

To summarize, the DOE classification system is separate from, though closely linked to, the DOE security system, and is centralized. Classification policy originates in the Office of Classification. DOE is the Executive Branch agency with sole responsibility for Restricted Data. It makes extensive use of classification guides in order to bring about consistency in classification determinations throughout the Department.

4.2 HISTORY OF PROLIFERATION

The U.S. developed the world's first nuclear weapons in 1945, over a period of less than four years and at an expense of more than $2 billion. The first "proliferation" of nuclear weapons occurred when the Soviet Union successfully tested a fission explosive in 1949. U.S. efforts to develop a "hydrogen bomb" began during World War II, but at a relatively low level until an official decision to proceed was made in January 1950. The first successful thermonuclear detonation was achieved by the U.S. in October 1952, and by the Soviets in 1955. Table 2, below, gives a capsule summary of known (tested) proliferation to date.

TABLE 2

CHRONOLOGY OF PROLIFERATION

Country	Fission Test	Thermonuclear Test
U.S.	1945	1952
U.S.S.R.	1949	1955
U.K.	1952	1957
France	1960	1968
China	1964	1967
India	1974	--
Israel	?	
South Africa	?	
Pakistan	?	
North Korea	?	
?	?	

Lessons Learned

The United States carried out the atomic bomb project under a mantle of military security where essentially all information was classified. While some information was declassified after World War II, the Atomic Energy Act of 1946 continued extremely tight controls on weapons information in order to maintain the U.S. monopoly as long as possible. Despite these strict classification and security policies, the Soviet Union detonated their first fission device in 1949, four years after the U.S., and several years earlier

than had been expected by U.S. experts. It has been estimated that Soviet espionage against the U.S. Manhattan Project saved their fission bomb program at least two years.

As shown in Table 2, the United Kingdom became the next nuclear weapon country in 1952 and France followed in 1960. However, some other countries (such as Canada, Germany, and Japan) which had the technical capability and the nuclear material have decided to forego a nuclear capability. It can be concluded that:

- A technically advanced country with adequate resources, nuclear material, and a political commitment can eventually develop a nuclear weapon despite classification and security programs intended to prevent such proliferation. An ever-increasing number of countries (e.g., Iraq) should now be considered technically competent to develop nuclear weapons.

- Some technically advanced countries have elected not to undertake a nuclear weapons program, even though they possess the necessary technology and material. However, they can still contribute to proliferation by others through the publication and transfer of nuclear weapons-related technology.

The Chinese weapons program advanced at a relatively rapid rate in both the development of fission and thermonuclear weapons. The Chinese tested their first fission device in 1964, which was followed in a relatively short time by a thermonuclear test in 1967. This may, in part, reflect the assistance they are reported to have received from the Soviets in the production of nuclear material and in weapon design and production. The Chinese, in turn, appear to have provided support in nuclear technology to Pakistan and other countries. The Iraqis have received technical help from a variety of sources. It can be concluded that:

- The U.S. classification system can have little influence in preventing nuclear proliferation without the cooperation of other

countries, especially nuclear weapon states, in controlling information that would be useful to a potential proliferant.

The French thermonuclear weapons program proceeded at a relatively slow pace. While the French tested their first fission device in 1960, it was not until 1968 that their first thermonuclear device was tested. Bertrand Goldschmidt, a French scientist who worked in their nuclear program, states in his book "The Atomic Complex" that if the French had known in the 1960s the (then highly classified) "secret of the H Bomb" as published in the Progressive Magazine in 1979, it would have saved them several years in their thermonuclear bomb program.

- Even though classification may not be able to prevent a determined country from acquiring a first-generation nuclear weapon, it can significantly delay the time at which more advanced nuclear weapons are acquired. A resource-and time-consuming development program, and potentially revealing tests, are required to turn general concepts into a sophisticated thermonuclear weapon capability.

It has been alleged that Israel benefited from foreign assistance (governmental and other) in its nuclear program, including assistance from France and the United States. For example, a number of Israeli scientists studied fuel reprocessing and plutonium fabrication, among other subjects, at U.S. facilities between 1955 and 1965. The London Sunday Times in October 1986 published purported details of the Israeli nuclear program provided by a former worker at the Dimona nuclear complex. According to Dr. Theodore Taylor, a former U.S. bomb designer, the photographs indicate that Israel's nuclear program is far more sophisticated than previously believed.

India's nuclear program also benefited from the assistance of a number of countries, including the Soviet Union and the United States. Canada supplied India with a large natural uranium-fueled, heavy water-moderated, research reactor (CIRUS) and the initial fuel load. The United States provided the heavy water for the reactor. This reactor was covered by pledges of no

military use. However, CIRUS was the source for the plutonium used by India in its test of a "peaceful nuclear explosive" device in May 1974.

- The effectiveness of U.S. classification policy in preventing proliferation can be seriously undermined by various forms of assistance to proliferating countries from other countries, particularly nuclear weapon states, including the United States.

As a result of U.N. inspections following the Persian Gulf war of 1991 it was learned that Iraq was using electromagnetic calutrons to separate uranium isotopes as a means to acquire highly enriched uranium for their nuclear weapons program. Calutrons were used by the United States to enrich uranium for the first uranium bomb. The calutron was declassified in the 1950s because it was believed to be unlikely that such an inefficient and expensive system would be used by other countries to enrich uranium, and because Denmark had already constructed a calutron and described its construction at an unclassified symposium. Accordingly:

- Classified information considered to be obsolete by U.S. standards may still be useful to a potential proliferator and therefore should be declassified only if it is no longer protectable, or there is a compelling reason to do so. This is especially important for older nuclear weapon designs and isotope separation methods. However, such a policy by the U.S. can only be effective if other countries who have similar information also protect it.

The Atoms for Peace initiatives that were included in President Eisenhower's speech to the United Nations in 1953 led to declassification actions that were intended to foster a civilian nuclear industry in the U.S. Civil power reactors, nuclear fuel fabrication, and nuclear fuel reprocessing were among the program areas that were declassified. In this case, national policy influenced the direction of RD declassification that resulted in making information available (especially fuel reprocessing) that proved extremely useful to proliferant countries. For example, the plutonium used in India's nuclear device detonated in 1974 was recovered from reprocessed nuclear fuel.

- Declassification actions can further national policies that are based on legitimate national interest, but they may also make available information that will later prove to be useful to a proliferant country.

For first-generation nuclear weapons, much of the necessary general technical information has already become available, so the availability of nuclear materials and certain manufactured items and specialty metals are probably the controlling factors for a proliferant country. For example, it is estimated that export controls have probably slowed Pakistan's nuclear program by at least 5 years. Dr. A. Q. Kahn, a Pakistani who was employed on the URENCO gas centrifuge project, remarked about U.S. efforts to delay the Pakistan nuclear program: "Tremendous pressure was brought on us, our economic aid was cut off by the USA, embargo was put on such small things as rubber O-rings, magnets, and maraging steel." Note, however, that Pakistani officials recently confirmed that they now have a near-term nuclear weapon capability.

- Export controls on materials and equipment may be more effective than classification in delaying initial nuclear proliferation.

It must be reemphasized that neither classification nor export controls can prevent proliferation. Once a decision to commit the necessary resources has been made, these measures can only serve to delay a proliferator. Diplomacy, economic sanctions, or any other means of persuasion must play a key role in restraining proliferation.

The primary restraint on proliferation in the long-term is international cooperation: political, military, and economic as well as common standards for restraints on nuclear weapon-related technology, including production of fissionable materials.

4.3 THE FUTURE ROLE OF CLASSIFICATION

The purpose of this section is to provide a conceptual framework for a long-term approach for classification policy over the next few decades. Central to this discussion is the likely role of classification in protecting U.S. military nuclear capability, including restraining future proliferation.

The preceding historical survey emphasizes that the knowledge required to construct a nuclear device is not confined to nations currently possessing nuclear weapons. The primary reason that proliferation has not proceeded even more rapidly is that a number of nations technically able to develop nuclear weapons have made political decisions not to do so, not because of U.S. (or other) classification and export controls. In this context, classification is only one of the many tools of the overall nonproliferation policy of the United States, and must always be viewed in that larger context.

The history of proliferation indicates that the technical capability for proliferation has increased internationally through a wide variety of channels outside of classical espionage or clandestine acquisition of information, nuclear materials, or manufactured items. These channels of proliferation include nation-to-nation aid, unclassified technical interactions such as conferences, hiring by proliferators of foreign-born or foreign-educated technical experts, technical education of foreign students, systematic study of the unclassified literature (e.g., declassified information), and acquisition of commercially available technology. Perhaps the most important factor, over the long term, has been the inevitable international spread of technical and scientific knowledge with time.

In the present world, it is clear that the dissemination of technologies relevant for proliferation continues to occur at the international level, to a large extent independent of U.S. classification policy. For example, the considerable progress of Iraq toward becoming a nuclear power was largely independent of U.S. classification policy.

The above observations do not mean that present efforts to classify information relevant to proliferation are futile. Classification increases the time, cost, and uncertainty for a proliferator to construct an initial nuclear device. This provides more time to detect efforts at nuclear proliferation and to apply international pressure to restrain such attempted proliferation. Marginal delays in a nuclear weapons development program could be crucial in some instances. If, for example, Iraq had had several operational nuclear weapons, Operation Desert Storm might have taken a very different course.

It is important to note that significant upgrading of an existing nuclear capability is also a form of proliferation. Classified information (e.g., detailed modern weapons designs) which might not be of immediate use to an initial proliferator could be extremely important to an existing nuclear power seeking a higher level of technological sophistication in its nuclear weapons. Detailed design information could also be of use in developing more sophisticated and effective countermeasures to U.S. nuclear warheads.

There is often no clear line of demarcation between information useful for first-time proliferators and for those seeking to upgrade an existing capability. For example, high-performance computing and sophisticated software (particularly if validated by a nuclear weapon state) could be of great value not only in development of advanced nuclear weapons but also in increasing the level of confidence that a primitive nuclear device would work in the absence of testing or with minimal testing.

For the foreseeable future, classification will continue to serve several key objectives: delaying proliferation (initial or upgrading), protecting U.S. nuclear weapons from unauthorized use, and minimizing the possibility of developing effective countermeasures. All of these objectives help buy time for political solutions at the international level to the long-term threat of nuclear weapons, including proliferation.

Two long-term U.S. goals that are affected by classification policy can only be achieved through international cooperation:

- A high degree of assurance of the safety and use control of foreign nuclear weapons against unauthorized or accidental detonation.

- Control of nuclear weapons through international agreements, including limiting proliferation and the substantial reduction of all weapons in international inventories.

These goals will probably require some government-to-government sharing of information which is currently, and should remain, classified. In the case of nuclear weapons safety and use control, the U.S. might wish to transfer some relevant technologies which are currently classified to other nuclear nations. The risks inherent in such transfers could be determined to be greatly outweighed by substantial gains in the safety and security of nuclear weapons.

Effective control of nuclear weapons will involve verification of controls on proliferation and verification of nuclear material and weapons inventories. Particularly at lower inventories, this will probably require greater levels of controlled international access to information that is currently classified. Increased access to classified information would be likely, for example, from intensive on-site inspections and increasingly sophisticated technical procedures for verification. This long-range general forecast for the future international environment puts a premium on a classification system which is sufficiently flexible to allow for such increased sharing of carefully limited classified information. The RD system, in its current form, does not have this flexibility.

For the foreseeable future, nonproliferation will remain a central goal of U.S. national security policy. The primary lesson of the history of proliferation, as it relates to classification, is that international cooperation on classification policy is essential if U.S. classification policy is to continue to be a significant means of restraining proliferation

in the future. It does little good in the long run for the U.S. to attempt to protect technologies with strong implications for proliferation if those technologies are not being similarly protected by all nations possessing them, whether nuclear powers or not.

A final observation is that national security is now being interpreted in a broader context than before. Nations that fail economically cannot indefinitely maintain a strong national defense. The original RD system was founded with the premise that the inherent penalties and costs of classification were not a major consideration due to the overriding initial imperative to maintain the nuclear monopoly of the United States, and then later to maintain a qualitative U.S. advantage in nuclear weapons technology. Classification policy decisions must now be made in the context of increased priorities for such other broad national objectives as commercialization of technologies developed by the government, environmental cleanup, and overall government efficiency.

5. FINDINGS AND RECOMMENDATIONS

This section presents information and opinions obtained from interviews, historical research, and other sources. These findings are used as a basis for identifying issues and alternative options for actions to improve the DOE classification system. Those issues and options which were deemed to be most important have been selected for discussion. Major issues were identified in two general areas: the form or basic structure of the classification system, and classification policy concerning the content and operation of the system (i.e., which information should be protected and how). The study makes seven major recommendations for action. The first six involve structural changes. The final recommendation involves suggested changes in DOE policy. The study also makes a number of suggestions or observations. These differ from the recommendations in that they are more narrowly focused, or involve areas that do not require near-term action or are only associated with classification, such as information security.

5.1 ALTERNATIVE CLASSIFICATION SYSTEMS

One major focus of this study is on the institutional character of the Restricted Data (RD) system as mandated in the Atomic Energy Act (AEA) of 1954, as amended. Will the statutory RD system remain adequate and appropriate for the coming decade, and beyond? This question was the principal subject for analysis.

5.1.1 Alternative Forms

A number of alternative systems for classification of the technology of nuclear weapons and other military uses of nuclear energy are conceivable. These alternatives form a continuum -- ranging from termination of the RD system and declassification of everything now contained within it -- to replacement of both the RD and NSI systems with a new statute-based classification system combining the best features of each.

Classification obviously cannot, by itself, stop proliferation. However, it is equally obvious that declassifying all present Restricted Data would make the detailed designs of nuclear weapons and all nuclear weapons-related technology (including production of enriched uranium and plutonium) readily available to potential proliferators. This information was developed by the U.S. over more than 45 years, at a cost of more than $100 billion. Providing this information would make proliferation (including upgrading existing capabilities) much easier, faster, cheaper, and less uncertain. For example, the need for nuclear tests would be reduced. U.N. inspections have shown that Iraq had a sophisticated nuclear weapons program, and was probably within a year or so of attaining a nuclear weapons capability. Had sufficient classified information (on centrifuge technology, for example) been available early enough to Iraq, they could well have had operational nuclear weapons before the Gulf War.

Complete declassification of RD is clearly not consistent with current or conceivable future U.S. national security. Some military nuclear information must be protected, as effectively as reasonably possible, and therefore some classification system is necessary. The question is what form would be best?

A new statute-based system covering both RD and NSI information could, in principle, have much to recommend it. However, to determine the merits of this approach would require an interagency study well beyond the scope of the present effort. This alternative, therefore, received no further consideration here.

This leaves a number of practical alternatives to be examined more fully. The focus in this and in the following subsection is on the form of the system to be used to define classification, not on its specific content. Content is examined in Subsection 5.3, below. The information itself can, in principle, be classified under any system.

Four possibilities for alternative classification systems were considered:

1. Retain the current RD system with no structural changes.

2. Retain the current RD system, but with appropriate legislative or other structural modifications.

3. Discontinue the current RD system and use the NSI system for all RD information.

4. Replace the RD system with a new statutory system.

Alternative 1 - Retain the current RD system with no structural changes.

This alternative reflects the judgment that nuclear weapons are uniquely destructive, RD information remains sufficiently sensitive to justify a separate system for classification, and that the special features of the present RD system such as "born classified" provide especially useful tools for slowing nuclear proliferation.

This alternative argues that the present system is already sufficiently flexible to allow consistency with the previous guiding principles without amending the Atomic Energy Act. Amendments to the Act would not be entertained until they become clearly necessary to deal with immediate and pressing specific needs -- such as increased need for international cooperation to verify arms control treaties or to restrain proliferation. Increased comparability with the NSI system would be desirable, but only to the extent it is consistent with a high level of protection of sensitive nuclear weapons information and can be justified on the basis of decreased costs. The unique destructiveness of nuclear weapons suggests the need for a cautious incremental approach. Regulatory or administrative changes could be made as needed to help facilitate domestic initiatives such as technology commercialization, environmental cleanup, and facilities reconfiguration.

Arguments for:

- Requires no legislation.
- Leaves unique features of RD (such as "born classified") in place.
- Maintains the stability of a statutory system.
- Ensures centralized control in establishing systematic, consistent classification policy for military nuclear information.

Arguments against:

- Maintains strict controls on international exchange of RD information that hamper international cooperation on non-proliferation and arms control, particularly in establishing common international standards for controls on nuclear weapon technologies, e.g., common policies for classification. Disregards the new opportunities and the needs for increased international cooperation due to, for example, the breakup of the Soviet Union and the aftermath of the Persian Gulf war.
- Forgoes any cost savings that could result from a single, government-wide classification system.
- Allows no adjustment for statutory features that have lost utility with the passage of time.

Alternative 2 - Retain the current RD system, but with appropriate legislative or other structural modifications.

This alternative reflects the view that nuclear weapons remain uniquely destructive, and that those features of the current RD system that best support nonproliferation goals should be retained. However, structural changes such as appropriate amendments to the AEA would be sought to increase

the flexibility of the RD system, particularly to facilitate carefully limited sharing of RD information with selected foreign countries for the purpose of increasing international cooperation in such areas as restraining proliferation, enhancing the safety of existing nuclear weapons, combating nuclear terrorism, and restricting and reducing nuclear inventories through arms control agreements. The current AEA permits sharing of nuclear weapons and military reactor RD only for purposes of mutual defense. It has virtually prohibited any U.S. sharing of nuclear weapons RD except with the UK and, to a much lesser degree, with France and other NATO members.

Arguments for:

- Retention of the RD system emphasizes continued U.S. concern about nuclear proliferation.

- Maintains the stability of a statute-based system.

- Ensures centralized control in enforcing systematic, consistent classification policy for nuclear information.

- Allows greater flexibility in international exchange of RD information. Present controls hamper efforts to cooperate on non-proliferation, arms control, combating nuclear terrorism, and safety of nuclear weapons.

- Congress is more likely to modify the RD system than to discard it.

Arguments against:

- Forgoes improved efficiency (e.g., cost savings) that could result from a single uniform classification system.

- The recommended legislative changes could require considerable time to get the approval of Congress, while some of the needs are immediate.

Alternative 3 - Discontinue the current RD system and use the NSI system for all RD information.

This alternative reflects the judgment that nuclear weapons information is no longer unique and more sensitive than many other categories of defense information, and therefore no longer requires a separate classification system. This NSI approach is more flexible, and could accommodate a wide range of institutional controls on information, ranging from a strictly compartmented special-access NSI subset within DOE (operationally similar to the present RD system), to an uncompartmented system like that used for most NSI information. This alternative reflects the judgment that, in view of the flexibility offered by the NSI system, termination of the RD system and use of the NSI system would be the most straightforward way to adopt a common flexible national system for classification.

Arguments for:

- Would permit increased international cooperation on nonproliferation, arms control, combating nuclear terrorism, and nuclear weapons safety through selective sharing of classified information under current NSI procedures.

- Executive Branch would have greater flexibility to adjust nuclear classification policy to fit both domestic and international objectives.

- Possible long-term cost savings of a single government-wide classification and security system.

- If a strict special compartmented system is used, would continue to recognize nuclear information as especially sensitive.

Arguments against:

- Could be interpreted by other nations as a signal of reduced U.S. concern over proliferation.

- The relative stability of a statute-based classification system would be lost.

- While nuclear information would still be closely controlled, the advantages of present RD features such as "born classified" would be lost.

- Would involve substantial costs for conversion, and if not carefully implemented, DOE operations might proceed essentially the same as with RD (i.e., might seem little more than a change of name).

- Congress would need to be convinced to abandon a system of their creation, and leave implementation to the Executive Branch.

Alternative 4 - Replace the RD system with a new statutory system.

The RD system would be replaced with a new statutory system for classification of nuclear weapons and weapons-related information. Sections of the Atomic Energy Act dealing with classification would be repealed, and an entirely new classification system enacted either as a new section of the Act or as independent legislation.

This alternative would reflect the judgment that crafting all-new legislation provides somewhat more flexibility in achieving nonproliferation and other objectives than modification of existing legislation as under Alternative 2.

Arguments for:

- Maintains the stability of statute-based system.
- Reemphasizes U.S. concern about nuclear proliferation.
- Allows new legislation to be designed from the beginning to take into account current national and international conditions.
- Provides a visible symbol of DOE determination to make serious improvements in its classification system for nuclear weapons and military reactors.

Arguments against:

- Unless the new statute also extended to NSI, this alternative would forego any cost savings that could result from a single uniform government-wide classification system.
- Would entail added administrative costs for converting guidance, markings, regulations, etc., to new terminology and procedures.
- Congress would have to be convinced of the merits of a new statute as an alternative to limited amendment of the AEA.

5.1.2 Comparison of Alternatives

Alternative 1 would retain the current RD system. In view of the increased opportunities for more effective international cooperation on nuclear weapon issues, and the continued long-term threat posed by nuclear weapons, it is difficult to justify this essentially "business as usual" approach. The need for change seems compelling. Accordingly, Alternative 1 was rejected.

Alternative 4, a completely new statute, is basically equivalent to extensively amending the AEA. It would be preferable only if, for some

reason, amendment of the AEA would be more complicated or the resulting system would be less flexible. It is difficult to see why this would necessarily be the case. Amendment of the AEA would almost certainly seem less drastic to Congress and preferable to developing a completely new statutory basis for protecting nuclear information. Accordingly, Alternative 4 was also rejected.

Alternative 3, changing to the NSI system, appears to offer some advantages over merely modifying the current RD system. The NSI system already has flexibility for selective international cooperation, and a single government-wide classification system would probably simplify government operations. However, NSI is most often used to protect not technology, but its application to weapon systems (along with information concerning military operations, foreign policy, and intelligence). The NSI system is also, in principle, subject to change at any time by the Executive Branch.

Alternative 2 would retain the current RD system, but with appropriate structural (e.g., legislative) modifications. The RD system was designed primarily to protect the technology related to nuclear weapons and military reactors, as well as its application to specific deployed systems. Moreover, the clear-cut single agency authority, the centralization of classification policy development and declassification actions at a high level, the requirement for special consideration before classified information is shared with other nations, and the stability of a statutory system all make the current RD system appropriate for dealing with such highly destructive technology.

In the RD system all technology in the appropriate areas, whatever its origin, is classified until officially declassified, i.e., it is "born classified." NSI, on the other hand, is government information which requires a positive action to classify it, and generally involves information concerning technology that has been developed to the stage of application in specific systems. The RD system "born classified" feature often protects technology better than NSI, particularly in the early stages before its significance may be clear. While the inevitable diffusion of technology might be expected to

reduce its importance, the great majority of those interviewed felt that the "born classified" approach was still valuable.

Alternative 2 also has another very important advantage over Alternative 3. It would avoid major disruption in DOE operations by retaining the basic framework which has worked well for 45 years. It should also be easier to get Congress to modify the RD system than to abandon it. Congressional staff interviewed felt that even modification of the AEA would require making a very convincing case.

5.1.3 Recommendation

On balance, the Restricted Data classification system should be retained, but with appropriate legislative or other structural modifications to make information management more flexible and more credible (i.e., Alternative 2). The threat of nuclear weapons, including proliferation, remains a paramount concern and is the primary reason for maintaining a separate classification system for nuclear weapons, military reactors, and related information.

The RD system provides, on balance, the best way to buy time for eventual political solutions. Current increased proliferation concerns make this an inappropriate time to abandon the statute-based system of RD classification provided by the Atomic Energy Act. Any future decision in favor of a common government-wide NSI classification system could be made on the basis of experience under the modified RD system.

- **Recommendation 1: Retain the current Restricted Data system, but with appropriate structural modifications.**

5.2 STRUCTURAL CHANGES TO THE CURRENT RESTRICTED DATA CLASSIFICATION SYSTEM

A number of structural changes would help make the RD system more effective and more flexible in responding to a rapidly changing environment. The most obvious way to change the form of the system is through appropriate legislation. However, in view of the serious reservations many people have concerning amending the AEA, all possible alternative regulatory, administrative, and other non-legislative ways to accomplish these objectives should be carefully evaluated. In some cases other alternatives may be identified that turn out to be preferable. The recommended structural changes would also have the effect of making the RD system more operationally comparable to the NSI system used for all other classified information.

5.2.1 Arms Control and International Cooperation

By design, the present RD classification regime severely limits U.S. possibilities for communication to other nations of information on nuclear weapons, methods for production of SNM, and military reactors. Communication of any Restricted Data internationally can, under present law (sections 123 and 144 of the AEA, see Appendix D), be done only under terms of a Congressionally-reviewed Agreement for Cooperation. RD on nuclear weapons or military reactors can be communicated only in connection with a mutual defense agreement (or, in principle, other Congressionally-approved "international arrangements"). Transfer of such information for any other purpose can only take place if the information is removed from the RD category.

An urgent and very serious U.S. national security concern in the coming months and years is the control of the tens thousands of (formerly) Soviet nuclear weapons. The breakup of the Soviet Union has brought into sharp focus the critical nature of nuclear weapon command and control authority. Positive control over these nuclear weapons, wherever they may be located, is a major concern of the United States. It would appear to be of major importance to establish a future ability to discuss this issue with Russia and other states of the former Soviet Union. An example would be to exchange information on

certain aspects of nuclear weapon control/use-denial systems such as permissive action links.

In this connection, President Bush on September 27, 1991 called for cooperation with the (former) Soviet Union on control of nuclear weapons:

> "During last month's attempted coup in Moscow, many Americans asked me if I thought Soviet nuclear weapons were under adequate control. I do not believe that America was at increased risk of nuclear attack during those tense days. But I do believe more can be done to insure the safe handling and dismantling of Soviet nuclear weapons. Therefore, I propose that we begin discussions with the Soviet Union to explore cooperation in three areas: First, we should explore joint technical cooperation on the safe and environmentally responsible storage, transportation, dismantling, and destruction of nuclear warheads. Second, we should discuss existing arrangements for the physical security and safety of nuclear weapons and how these might be enhanced. And third, we should discuss nuclear command and control arrangements, and how these might be improved to provide more protection against the unauthorized or accidental use of nuclear weapons."

On November 27, 1991, the U.S. Congress responded to the same urgent concerns by passing the "Soviet Nuclear Threat Reduction Act of 1991" (SNTRA), which authorized expenditure of up to $400 million to support cooperation with the Soviet Union, its republics, and any successor entities to:

- Destroy nuclear weapons, chemical weapons, and other weapons.
- Transport, store, disable, and safeguard weapons in connection with their destruction.
- Establish verifiable safeguards against the proliferation of such weapons.

It is very important that the classification system for nuclear weapons be sufficiently flexible to allow carefully limited exchange of any information which may be required for effective cooperation.

More generally, some in DOE, State, and the Arms Control and Disarmament Agency (ACDA) believe that selective communication of certain carefully limited RD information would be in the national interest. Such information would not need to contribute substantially to the nuclear weapons capabilities of other nations in order to support such national objectives as arms control, development of international guidelines for classification and other measures for control of nuclear weapons-related technology, development of international responses to nuclear terrorism, as well as useful exchanges on nuclear weapon safety and security.

Arms control is a particularly important area which is affected by current limitations on communication of RD to other nations. Negotiation and effective verification of arms control agreements leading to substantial reduction of nuclear weapons would benefit from the ability to share a limited amount of information currently classified RD/FRD with Russia and perhaps other nuclear weapon states (e.g., during Special Access Visits under the START treaty). This information would be designed to contribute very little to their current nuclear weapon capabilities. However, under current law, exchange of such RD could only be done in connection with mutual defense agreements, or under explicit provisions in a treaty, or by declassifying such information and thereby making it available to all. Because the information exchange expected could potentially reveal specific information on nuclear weapon design, declassification would not be consistent with nonproliferation goals.

Another important area where exchanges of limited RD could facilitate international cooperation is in developing common worldwide standards for control of nuclear weapons-related technology. U.S. controls, alone, can no longer have much effect on proliferation. The widespread diffusion of technology means that common international standards are urgently needed for protection of nuclear weapon-related technology. U.S. classification policy

must be sufficiently flexible to facilitate international discussions to arrive at common policies for control of nuclear weapons-related information, materials, and equipment.

Observation 1: ***High priority should be given to efforts to arrive at common international standards for classification and other controls on nuclear weapons-related technology.***

There are several possible ways to facilitate communication of limited amounts of RD information on nuclear weapons technology for purposes of international cooperation on controls of nuclear weapons. The most direct way is to amend the AEA.

One option which does not require amendment of the AEA is that of a Congressionally approved treaty, Executive Agreement, or other international arrangement. Carefully drawn treaty language spelling out specific information to be exchanged could provide a mechanism for communication of RD. In the case of the former Soviet Union, the Soviet Nuclear Threat Reduction Act of 1991 may, arguably, authorize exchange of RD as needed for its purposes.

Declassification is another option. Declassification of certain general qualitative RD information could be helpful in specific cases. One possible example is general information concerning potential terrorist nuclear devices. Another is a more complete description of which materials can be used in nuclear explosives. However, declassification of the necessary information could, in many cases, lead to an unacceptable increase in the risk of proliferation, clearly not in the interest of any party to the exchange.

All other options would appear likely to require changes to the Atomic Energy Act. One option would be to eliminate RD entirely, bringing all nuclear-related information under the NSI Executive Order. It could then be communicated under present NSI procedures, i.e., through the Presidential National Disclosure Policy and the associated interagency National Disclosure Policy Committee. This would provide maximum flexibility to the Executive

Branch. A more limited form of this option would allow transclassification to NSI of only the specific information to be communicated. However, this latter approach could lead to later confusion over the proper domestic classification of such RD material which had been transclassified in a limited foreign transfer context.

The preferred option is to modify the Atomic Energy Act to allow selective, timely, communication of carefully limited RD for the purpose of international cooperation in arms control, countering nuclear terrorism, or nonproliferation. The criteria should be drawn sufficiently broadly to allow the Secretary of Energy, in coordination with appropriate executive and legislative branch authorities, to determine that communication of specific limited RD would benefit national security and accordingly to authorize the communication. (Note that the Secretary of Energy is already responsible for managing RD, including declassification of RD.) This could preserve traditional Congressional policy and oversight prerogatives and yet would permit the United States to respond to rapidly changing and quite complex national security objectives in the present world situation.

Recommendation

Provisions should be made for limited communication of RD to selected foreign countries under carefully prescribed conditions when it is necessary to achieve U.S. national security goals such as enhancing the safety and security of nuclear weapons, verifying arms control agreements, implementing effective international controls on nuclear weapon technology, or countering nuclear terrorism.

- **Recommendation 2: Amend the Atomic Energy Act to allow the Secretary of Energy, in coordination with appropriate executive and legislative branch authorities, to approve communication of carefully limited Restricted Data to selected nations for the purposes of more effective cooperation on arms control, nonproliferation, combating nuclear terrorism, and nuclear weapon safety.**

Implementation Options

One possible approach would be to add a new subsection "144 e." to the AEA providing the Secretary of Energy authority to communicate limited RD for the purposes of international cooperation in arms control, nonproliferation, combating nuclear terrorism, nuclear weapon safety, and perhaps other stated purposes, with appropriate notification of Congress. The SNTRA would, at most, allow RD to be communicated to the former Soviets for purposes related to dismantlement of their weapons.

Declassification can be of only limited use in accomplishing the objectives of Recommendation 2. However, current classification of general, qualitative information on nuclear weapons technology should be carefully examined to see to what extent selective declassification could help international efforts to control nuclear weapons technology. Possible areas include more specific identification of nuclear weapons-usable materials and other generic information in areas of nuclear weapons technology that should be subject to international control.

5.2.2 Military Utilization Information - Formerly Restricted Data (FRD)

Another useful revision to the AEA would be elimination of the category of information known as Formerly Restricted Data (FRD). The Act does not use this term; it was coined by the Atomic Energy Commission to describe a category of information identified in sec. 142 d. of the AEA which is concerned primarily with the military utilization of nuclear weapons, including such information as numbers, yields, and locations of nuclear weapons. Properly defined, FRD is information that reveals little about weapons design, but is essential for military planners. Within the United States FRD is treated like NSI. Access to FRD requires only clearance for access to NSI at a comparable level of classification. For overseas communication, however, FRD is treated as RD and can only be shared with allies and under an Agreement for Cooperation.

Many of those interviewed had little contact with FRD. Many also commented on the misleading character of the FRD designation; i.e., "Formerly Restricted Data" is not RD that is no longer classified. Most of those with experience in dealing with FRD believed that such information would be better handled everywhere as NSI, and that the appropriate level of classification in any specific instance would be best determined in consultation with the DOD.

Elimination of FRD would offer some advantages:

- Would eliminate the requirement for an Agreement of Cooperation for international communication of military utilization information, increasing flexibility in responding to new conditions.

- Would resolve any operational problems encountered by NATO military forces because of special handling requirements for U.S. FRD transferred to NATO.

- Would simplify personnel clearance procedures for one category of classified information for which special requirements now exist.

- Would eliminate the Formerly Restricted Data terminology and the confusion that has resulted from its use.

- Would eliminate an overlap of the RD and NSI systems.

There would also be some disadvantages:

- Would require a sizeable administrative effort to revise classification guides, orders, and regulations, and change markings on documents.

- Congressional support would be required.

- Unless information to be transferred is carefully defined, risks transfer of design-related information.

Recommendation

On balance, elimination of the FRD category would increase the flexibility of the RD system and simplify DOD operations with little penalty to national security, provided such military utilization information to be removed from the RD to the NSI system is appropriately defined.

- **Recommendation 3: Amend the Atomic Energy Act to eliminate the Formerly Restricted Data (FRD) category now used to identify military utilization information and transfer such information to NSI.**

Implementation Options

Revision of the AEA appears to be the only way to eliminate FRD. This would involve eliminating the provision in sec. 142 d. that transfer of such information to a foreign government (or regional association) requires an Agreement for Cooperation. Joint responsibility should be retained by DOE and DOD for determining which military utilization information should be transclassified to NSI or declassified.

5.2.3 Reclassification Authority

Declassification and publication of specific information is essentially irreversible. Once information is officially released and made publicly available, it can no longer be controlled. However, this does not apply to information which has not yet been made public. Under Executive Order 12365, Cabinet-level government officials can reclassify NSI information when it can effectively avoid damage to national security. Addition of a provision to the AEA to allow carefully controlled selective "reclassification" of sensitive

(and controllable) declassified RD information would be supported by many, but by no means all, of those interviewed. In particular, this would allow classification of significant new information in declassified fields where earlier blanket declassifications contained no provisions for classifying major new developments, i.e., "breakthroughs." In addition, reclassification could eliminate the need for other controls on some sensitive but now unclassified information (e.g., some Unclassified Controlled Nuclear Information).

The traditional position of the DOE General Counsel has been that once an area of RD has been declassified under sec. 142 of the AEA, information in that area cannot be reclassified (whether as RD, FRD, or NSI) unless there was some caveat in the original declassification action that would permit reclassification of new information under certain conditions. No such caveat exists in some significant past declassification decisions, such as those declassifying technology for civil power reactors or reprocessing spent reactor fuel. For example, even a major breakthrough to more easily, cheaply, and safely extract plutonium from spent reactor fuel could not now be classified, even though it would be of major importance to a proliferator. The Act does, however, provide some protection for certain categories of declassified RD information that are related to atomic energy defense programs, by allowing their recapture under limited circumstances as Unclassified Controlled Nuclear Information (UCNI) under the provisions of section 148 (see Section 5.2.5 below). In addition, foreign dissemination may be subject to export control.

A limited authority for the Secretary of Energy to reclassify RD information, subject to very stringent standards for application (similar to those for NSI), would offer some advantages:

- Would provide a tool for the protection for some declassified information that could be especially helpful to a proliferant.

- Would help to rectify previous classification decisions that were made without sufficient knowledge of future proliferation dangers.

- Would provide another way to satisfy one major objective of UCNI, i.e., control of particularly sensitive declassified nuclear weapon information.

Disadvantages include:

- Even a narrowly limited reclassification authority would be unpopular, and runs some risk of misuse. For example, there would be some risk of mistakenly reclassifying information that had already been widely disseminated.

- Congressional support would be required.

Recommendation

- **Recommendation 4: Amend the Atomic Energy Act to allow the Secretary of Energy under carefully prescribed conditions to reclassify specific information in areas of Restricted Data that have previously been declassified.**

Implementation Options

There are no present provisions in the AEA for "reclassification" of RD or FRD. A new sec. "142 f." could establish authority for reclassification of RD by the Secretary of Energy under stringent conditions for potential harm and practical effectiveness which would be similar to those which he must now meet for reclassification of NSI.

5.2.4 Non-Government Information - Private Restricted Data

Another suggested structural improvement for the AEA is the elimination of the present "private Restricted Data" feature by amendment of the Act to clearly define RD as only that RD-type information under government ownership or

control. The concept of "private RD" originates in the use of the adjective "all" in the AEA definition of Restricted Data; legal authorities differ over its meaning and effect. Many lawyers and groups such as the American Civil Liberties Union (ACLU) believe that if the Act attempts to control privately developed "Restricted Data" it is unconstitutional. DOE has historically taken the position that the Act does control privately generated information and is constitutional. For the most part, people interviewed felt that the concept of private RD was seldom used and had largely outlived its usefulness for nuclear weapons information, but that it could still have some value for controlling other RD information such as that dealing with isotope separation processes.

The authority to classify privately generated information as RD has been used on a limited basis by the government over the years since enactment of the AEA. The results have been mixed; in several instances involving isotope separation the privately generated information was successfully classified and controlled. In 1979 the government sought and received a preliminary injunction blocking publication in The Progressive magazine of purportedly privately generated classified information on general features of the hydrogen bomb. While under appeal, the case was mooted and publication followed. It should be noted that in this case -- the only existing court test -- a Federal district court decision supported government control of Restricted Data, independent of its source.

More recently, the concept of "reverse flow" of RD has arisen, in which the issue is U.S. control of private information of RD-character developed by foreign interests and introduced into the U.S. without a formal Agreement for Cooperation, and then used or modified by U.S. citizens and subsequently returned to foreigners. The URENCO (a U.K., Netherlands, and German consortium) centrifuge enrichment enterprise proposed to be located in Louisiana provides a specific example. This situation -- clearly never envisioned by the framers of the AEA -- presents difficult legal problems under the current legislation.

It should be noted that National Security Information excludes private information. Unlike RD, NSI information must be owned by, produced by or for the government, or be under the control of the government.

Several arguments support amendment of the AEA to eliminate private RD:

- The authority to control private RD is rarely used, and any deterrent effect is probably minimal, if not illusory.

- Would eliminate a provision of the Act whose constitutionality has been questioned.

- Would simplify dealing with foreign-developed "private RD" that is introduced into the U.S. (e.g., by URENCO) and used and possibly modified in the U.S. by U.S. nationals and then subsequently transferred back to the source nations.

- Other mechanisms (e.g., licensing, export controls, the Invention Secrecy Act) already exist for controlling the application of any genuinely privately-generated, proliferation-sensitive new technologies.

There could also be disadvantages:

- Loss of a deterrent to those contemplating publishing sensitive information -- however obtained -- pertaining to nuclear weapons, uranium enrichment, or other RD as a purported act of "public service."

- Congressional support would be required.

Recommendation

Possession or dissemination of special nuclear material, nuclear weapons, or production facilities are covered by other provisions of the AEA and other

legislation (e.g., licensing, export control, and the Invention Secrecy Act). Nuclear weapon "designs" invented independently by amateurs are not likely to be complete, correct, or credible. Important and unique details remain classified, although the basic concepts for production of special nuclear material and for design of nuclear weapons are largely available. Large-scale organized activities would be required for independent "private" development of significant, sensitive technology in either area. Presumably, the sponsors of such an effort would expect a financial return, either by sale of a product or service to the government, or by operation under government license. The government would therefore be able to retain control.

On balance, it is concluded that the private RD provision of the AEA is no longer useful. Under present circumstances the deterrent effect is questionable.

- **Recommendation 5: Amend the Atomic Energy Act to eliminate privately generated information from the definition of Restricted Data.**

Implementation Options

It has been suggested that implementation of this recommendation could be accomplished by a DOE policy statement published in the Federal Register stating that the Department no longer controls privately generated RD information. In view of the long history during which the Department claimed such authority and also used it successfully, the practicality of such an approach seems questionable.

It is also possible that some in Congress may insist that the Department has and should retain such authority. In that case, explicit congressional endorsement of private RD could go a long way toward restoring its value as a deterrent, particularly if it survives a direct court test.

Another possibility would be to avoid the literal interpretation of the AEA by defining thresholds below which DOE would have no interest. This has been done with isotope separation by declaring that DOE will regard a separation process that has little potential capability to produce significant quantities of special nuclear materials as unclassified. Application to weapons technology would appear to be less straightforward.

The simplest legislative option would probably be to amend the Atomic Energy Act by deleting the word "all" in the definition of Restricted Data and substituting in its place the word "government". This change could limit DOE to control of government RD information. Adequate justification would be required to convince some in Congress that this authority is no longer needed by DOE.

5.2.5 Sensitive Unclassified Information

The general issue of control of "sensitive unclassified" technology continues to complicate relationships between national security authorities and research scientists -- particularly in academia but also to some extent in industry and government laboratories. Researchers argue that truly sensitive information should be classified, and the basic concept of "sensitive unclassified" appears to them to be a contradiction in terms.

Many researchers believe that, in general, attempts to control dissemination of unclassified information will only stifle U.S. science and technology and international competitiveness. Computerized data bases (e.g., from DOE and NASA) were cited as examples that are becoming very important to the academic and industrial research communities. Controls over foreign access can only be effective if public access is denied. But this would mean that public and university libraries could not offer these data bases since they are not able to cope with the administrative burden of controlling access.

This is a legitimate concern. However, it must be balanced against the fact that full and free public release of commercially valuable scientific and technical information often precludes its rapid commercial development. Under

the recently passed legislation establishing Cooperative Research and Development Agreements (CRADAs) within DOE, the need to control unclassified but valuable technology was recognized by allowing for a 5 year exemption to the release requirements of the Freedom of Information Act. This delay in public release allows for the imposition of other, longer-lasting intellectual property controls on any valuable technology developed under a CRADA.

Controls on both technical and non-technical unclassified but sensitive information may be appropriate and acceptable depending on the reason for such controls. For example, controls based on personal privacy rights or financial or professional advantage may be more readily acceptable to some than controls based on national security.

Another legitimate concern is how reasonably an unclassified information control system is implemented. Its onerousness and rigidity should be in proportion to the sensitivity of the information with which it is concerned. If unclassified information control measures end up being essentially the same as those required for classified information, then it is legitimate to ask why it should not just be classified.

Universal application of classification to all currently unclassified but sensitive information is not the answer. For example, some of the physical protection requirements for Unclassified Controlled Nuclear Information (UCNI) may have been over-zealously applied by some so that UCNI begins to look like just another version of classified information. However, UCNI is designed to allow it to be shared (under certain conditions) with the private sector, e.g. for its potential commercialization.

Another similar example concerns DOE information bearing the Export Controlled Information (ECI) marking. Documents marked as containing DOE ECI are not available to anyone through the National Technical Information Service. Therefore, the DOE approach to denying this information to foreigners also denies it to much of the U.S. research and industrial community. However, complete loss of U.S. access is not necessary. The Department of Defense allows U.S. companies to have access to the DOD version of ECI by means of a

simple self-certification by the intended U.S. recipient company that it will "follow the rules." The primary enforcement mechanism in such a system is the threat of the loss of continued access to the desired information. Classification of such moderately sensitive information would have precluded such a flexible implementation.

There is clearly some unclassified information that would help potential proliferators and other malefactors if it were publicly available. UCNI and ECI are partial responses to a real problem. For example, "paper" and automated U.S. databases are of great interest to Iraq, Israel, Iran, Pakistan, and other countries, as well as to U.S. universities and industries. The challenge facing the DOE is to strike the proper balance between competing needs to limit yet selectively allow desired access to U.S. technology.

There should be a middle ground: U.S. interests are served by publishing of basic research results but limiting dissemination of sensitive, and protectable, technical know-how. These are already the goals of both the UCNI and ECI programs. The challenge is to assure that the day-to-day implementation of these and similar programs meets these goals.

Unclassified Controlled Nuclear Information (UCNI)

The category of Unclassified Controlled Nuclear Information (UCNI) was created by the addition of section 148 to the Atomic Energy Act in 1981. It was intended to limit access to sensitive unclassified information concerning the following: (1) design of facilities for SNM production or facilities for utilization of nuclear energy ; (2) security measures for their protection, and for the protection of nuclear materials in such facilities or in transit; and (3) previously declassified RD information concerning design, manufacture, or use of nuclear weapons. Such information is defined as UCNI if its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the public health and safety or the common defense and security by significantly increasing the likelihood of: (1) illegal production of nuclear weapons; or (2) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

At the time section 148 was passed, its principal purpose was to control information of potential use to a terrorist. It was not directed primarily at the problem of nuclear proliferation. Therefore, security information is more clearly within the scope of section 148 than is proliferation-related technology information. In addition, the description of which activities and facilities are covered by UCNI is not precise. This has complicated the generation of specific guidance in a number of subject areas.

The changing world political environment has increased the concern about nuclear proliferation. The scope of the UCNI program is being expanded to encompass unclassified proliferation-related technology in a number of subject areas. For example, UCNI controls are being considered for high explosive technology as applied to nuclear weapons, for plutonium processing, and for various types of isotope separation.

UCNI is objectionable to a variety of interest groups, who view it as primarily designed to frustrate Freedom of Information Act requests. UCNI is described by these groups, and by many within the DOE community (and by some on Congressional staffs), as too vague, and subject to misuse. The "adverse effects" criteria of section 148 of the AEA are not readily distinguishable from requirements for classification. No security clearance is required for access to UCNI, and the AEA specifies no criteria for access, yet imposes maximum penalties for improper dissemination (e.g., fines up to $100,000) that to many people appear dramatically out of proportion to the lesser penalties stipulated for the more serious offense of divulging RD.

Aside from the questions surrounding the criteria for access and for determining sensitivity, the most controversial -- although so far least used -- aspect of UCNI is the provision for protection of previously declassified weapon-related information. If DOE were given the authority to selectively reclassify key items of information, this provision in section 148 would be needed only in exceptional cases. The aspects of UCNI dealing with security can already be handled by classifying or reclassifying such information as NSI when classification is appropriate.

Amendment of section 148 of the Atomic Energy Act could ameliorate the most troublesome features of the current UCNI program while retaining protection for the sensitive unclassified information now identified as UCNI. The scope of the UCNI program could be clarified to allow proliferation-related technology to be controlled more effectively. In addition, the penalties for the release of UCNI should be brought into balance with those for the release of classified information.

Recommendation

The whole range of sensitive but unclassified information, including UCNI, needs to be more clearly defined to allow for the control of any unclassified nuclear technology of significant use to a nuclear proliferant. The penalties for misuse of UCNI are also disproportionate to the penalties for misuse of classified information. The following legislative action is suggested as a key step in improving the workability and level of protection afforded to this type of information.

- **Recommendation 6: Amend the Atomic Energy Act to better define the scope and enforceability of Unclassified Controlled Nuclear Information (UCNI).**

Implementation Options

This recommendation would require minor changes to section 148 of the AEA. Coupled with Recommendation 4 (reclassification authority), it would allow classification, where appropriate, and would also continue to provide protection for unclassified but sensitive nuclear information. Section 148 penalties for misuse of UCNI by government employees or contractors could be eliminated in favor of administrative penalties commensurate with other administratively controlled categories of information.

Other Categories of Sensitive but Unclassified Information: Export Controlled Information (ECI) and Official Use Only (OUO) Information

Export Controlled Information (ECI) is defined as unclassified government information whose foreign dissemination (export) is to be controlled due to its significant value for military or nuclear proliferation purposes. Such information, if developed in the private sector, would require an export license. DOE's Office of the General Counsel has taken the position that DOE does not currently have statutory authority to control ECI.

DOE has provided voluntary ECI guidelines to its Field Offices and laboratories. Some researchers regard this as unwarranted infringement of their rights to publish, even though the ECI designation is intended to be applied only to information pertaining to a process or product, and not to the publication of basic research results.

On two separate occasions the General Accounting Office (GAO) and Congressional committees have recommended that DOE obtain statutory authority to withhold ECI from FOIA requests, similar to the authority which DOD now has that is based on an Amendment to the 1984 DOD Authorization Act.

There are three options:

- Continue to rely on DOE and DOE contractors using the ECI guidelines on a voluntary basis to identify and control ECI information, or

- Develop a formal DOE ECI program based on an administrative control model rather than as a FOIA-exempt system, or

- Seek specific statutory authority from Congress to control ECI.

If U.S. export controls, particularly those on information and hardware relevant to proliferation, are to be effective, DOE needs the statutory authority to enforce the protection of such information developed within the

DOE complex. Development of a formal ECI program within the DOE, even if only an administrative control, could effectively control much ECI and help develop a basis for seeking needed legislation.

Another category of sensitive but unclassified information which requires protection is Official Use Only (OUO) information. OUO information is defined as sensitive, unclassified, but otherwise uncontrolled information which may be exempt from public release under the Freedom of Information Act (FOIA) if it falls within the scope of one of the FOIA exemptions, and if it is sufficiently sensitive that it should not be publicly released. DOE Defense Programs (DP) has published a DP Order (DP 5650.1) covering OUO, as has Security Affairs (SA 5650.1), and work is underway on a DOE-wide order for OUO.

Observation 2. ***Specific legislative authority is needed for DOE to withhold Export Controlled Information (ECI) from release under the Freedom of Information Act. In addition, formal procedures need to be established for a DOE-wide "Official Use Only" (OUO) Information Program.***

5.3 CHANGES IN DOE CLASSIFICATION POLICY

The preceding section proposed a number of structural legislative changes to the AEA which are designed to make the form of the classification system more flexible and more effective.

This section considers possible non-legislative changes in DOE classification policy concerned with the content and operation of the classification system. What information should be protected, taking into account the current national and international environment?

This study does not attempt to determine the level of classification appropriate for specific items of information. However, the study does suggest changes in classification in several broad areas which would better reflect current judgments of sensitivity.

First, the overall policy for what information should be classified is examined. A comprehensive fundamental review of all military nuclear information is proposed. Classification issues in a number of specific areas relevant to such a review are addressed in Sections 5.3.2 - 5.3.7:

- Environment, Safety, and Health
- Technology Commercialization
- Modernization and Reconfiguration
- Nuclear Weapons Development
- Information Security
- The Costs of Classification

Several suggestions and observations are made for changes in these areas. Possible ways to implement the suggested changes are then discussed in Section 5.3.8.

5.3.1 Overall Policy Concerning What Should Be Classified

The world has changed dramatically since the establishment of the RD system in 1946 when almost all nuclear information was classified. Over the years much of this information has been declassified, based on the AEA criterion of whether publication would cause "undue risk" to the national security. This involves balancing the degree of risk of harm from helping potential adversaries against the benefits of declassification to other national interests, foreign or domestic.

Evaluation of both risks and benefits changes with time. While U.S. interest in preventing the spread of nuclear weapons technology remains paramount, technological capabilities continue to spread worldwide. U.S. foreign policy and domestic priorities change and the emphasis on nonproliferation has sometimes been affected (e.g., the effect of the Soviet invasion of Afghanistan on U.S. treatment of Pakistan's nuclear program).

In the past few years, the pace of change has accelerated dramatically, e.g., the Persian Gulf war and the breakup of the Soviet Union. The political and military situation in the former Soviet Union has been changing rapidly. Proliferation concerns are becoming more central. The terms of worldwide economic competition are changing. Environment, safety, and health issues are assuming more importance everywhere, specifically in connection with DOE activities in environmental cleanup and modernization.

DOE classification policy needs to fully reflect the best current evaluations of both the benefits and the risks of declassification. Classification policy has changed greatly over the past 45 years as circumstances changed. However, current policy is based less on an overall coherent evaluation of present circumstances than on a succession of many major and minor declassification actions which have been made over the years to facilitate commercial nuclear power, to further general scientific and technical capabilities, to reflect independent publications, to improve programmatic effectiveness, and for many other individual reasons.

Many people interviewed said that there is now considerable over-classification. However, they were not in agreement on what should be downgraded or declassified. Some said that too much proliferation-related information had already been declassified, particularly by the U.S. Many believed that classification policy was overdue for a fundamental, top-to-bottom review to determine what information should be classified, and why.

In view of the recent enormous changes in the world political, economic and technical environment, it is time for DOE to conduct a systematic, fundamental, and comprehensive review of all nuclear weapon-related information to determine what should be classified, and at what level. This is a monumental task requiring high-level technical and policy judgments about both the risks and the benefits of publication. Undoubtedly, certain information now classified should be declassified. In addition, some limited amount of information in presently declassified areas may be so useful for proliferation that it should be reclassified (where public disclosure has not occurred) for better protection.

- **Recommendation 7: Conduct a comprehensive, fundamental review of all nuclear weapon-related information to determine what should be classified under present conditions, with the objective of removing from classification all information that no longer warrants such protection.**

Implementation Options

The recommended fundamental review is a major undertaking and would likely result in major declassifications. Such a review should involve both a wide range of technical expertise in nuclear weapons technology and a broad perspective on national security issues. Wide acceptability of the review would be greatly advanced by participation of appropriate experts from outside DOE. As discussed below, a fundamental review to reflect current sensitivity is likely to recommend major areas of declassification or downgrading, and

possibly specific upgradings, including more use of the Top Secret level, and even some limited reclassification if Recommendation 4 is implemented.

The new classification policy concerning what should be classified must then be reflected in the hierarchy of classification guides: the overall Classification Policy Guide, some 50 Program Guides, and hundreds of Local Guides. Due to the very close interaction between classification and security, current information security policy needs to be examined for corresponding changes needed to implement the suggested changes in classification policy. For example, more practical procedures may be needed for handling Top Secret RD. Classification policy and guidance need to be regularly reviewed, again with a broad range of expertise. To the extent possible, the costs of classification (both direct and indirect) need to be identified as one important consideration of what risk is "undue risk."

This study recommends that detailed classification judgments in specific areas should be made by a group of senior experts with a broad range of specific expertise. The following sections (5.3.2 through 5.3.6) give some suggestions and observations in several areas of current concern: Environment, Safety, and Health; Technology Commercialization; Modernization and Reconfiguration; Nuclear Weapons Development; and the connection between classification policy and information security. Section 5.3.7 discusses the importance and difficulty of establishing the true costs of classification. The final section (5.3.8) gives more detailed suggestions for implementation of the review process itself, as well as some illustrative examples of information which might be properly classified at each level, based on current sensitivity.

5.3.2 Environment, Safety, and Health

The Secretary of Energy has given high priority to building public confidence in DOE's environmental safety and health practices. To the extent possible this goal should be reflected in the Department's classification policy.

DOE facility wastes need to be described in sufficient detail to allow Federal, state, and local authorities to provide public assurance of regulatory compliance. Monitoring by cleared authorities is likely to be a short-term option, at best. Declassification may be required of inventories and production rates of wastes, and possibly of nuclear weapons, components, and nuclear materials. The association of particular materials with specific production plants (even specific buildings) may have to be declassified for purposes of environmental review. Note that declassification may not necessarily rule out continued protection from general public disclosure (e.g., under OUO or UCNI) in specific cases where the sensitivity remains sufficiently high.

Dismantlement of large numbers of nuclear weapons, now anticipated as a result of START and subsequent arms control agreements as well as from voluntary force reductions, may require disposal of some 80 separate materials, many not in current waste streams. Classified association of specific materials with particular weapons may be difficult to conceal with high confidence as the waste stream varies over time. An alternative to declassification -- secure storage of waste material in specially built facilities -- would be extremely expensive and might not, in the long term, provide a workable alternative to declassification. It might also hamper building public confidence in DOE's efforts to manage its environmental health and safety responsibilities.

Public interest groups are very concerned about these public health and safety issues. While some have acknowledged that there can be legitimate conflicts between public health and national security, they believe these should always be resolved in favor of the public's right to know. Some interviewees even argued that this right should be extended to public participation in setting capacity requirements for the new DOE complex, and therefore that information on the size and composition of current and planned nuclear weapons stockpiles should be declassified. Within the DOE complex, many interviewed believe that at least approximate values for the size of the nuclear weapons stockpile are no longer sensitive information and have no proliferation significance.

Security requirements to protect classified information tend to slow down progress and raise costs in DOE environmental restoration efforts. These requirements, in turn, generally stem from classification of wastes -- e.g., shapes, quantities, and compositions. Shapes, masses, and dimensions of weapon parts are generally classified. Compositions may reveal something about the materials used in weapons, and quantities can provide information on weapons materials inventories. Dismantlement of the lithium enrichment plant at Oak Ridge provides one example. It was asserted in interviews that disposal of the mercury-contaminated structure and machinery could reveal the total U.S. production for lithium enriched in Li-6. Even though production ended in the 1960s, the total amount produced is still classified.

Issues concerning public health and safety and effects on the environment arise in the following three principal areas of DOE operations:

- Management of hazardous wastes
- Production of weapons materials
- Weapons production, assembly, and disassembly

Management of Hazardous Wastes

Environmental restoration of plant sites where control of existing waste inventories may not be in compliance with current regulations (or is a source of potential risk to the public) cannot be impeded for very long by questions of classification. At some sites, DOE may still have the option of continuing the policy of classifying and storing by-product materials which would otherwise be categorized as waste. Waste compositions can reveal the use of specific materials in nuclear weapons. Sufficient quantitative information could allow estimation of production quantities or rates for weapons materials, weapons, or components.

A recent example involved finding traces of the hazardous material mercury-thallium downstream from DOE's Allied-Signal nuclear weapons facility in

Kansas City. This caused a major potential problem with EPA because at the time the mere association of mercury-thallium with the nuclear weapons program was classified. After careful evaluation, DOE decided to declassify not only the association of mercury-thallium with nuclear weapons program facilities but also the quantities present.

This example will undoubtedly be followed by many others. It may even soon be determined that nuclear debris buried deep underground from the hundreds of tests at the Nevada Test Site is "waste" subject to full EPA regulation. This "waste" could be monitored, as some wastes are today, by cleared Federal and state regulators. However, in the future, all waste management will have to be accomplished in compliance with EPA regulations, and probably with full public disclosure. In the longer term DOE must choose one of two options:

- Declassify specifications of all material identified as waste at DOE facilities, both in composition and quantity (possibly treating the most sensitive information as OUO or UCNI if the situation warrants), or

- Store classified wastes indefinitely on site, with appropriate security protection.

The first option -- declassifying waste -- would improve public confidence in DOE, allow publicly accountable disposal or storage, and should ultimately reduce the costs of operations. However, it could also, in some cases, enable reasonably accurate estimates of some material inventories and even weapon production rates. Material associations that are revealed may indicate that the U.S. has used some weapon design features not previously acknowledged.

The second option would require construction of secure storage facilities and the operational costs to maintain security, and may still not comply with all laws and regulations. For example, waste can no longer simply be put into the ground even in tanks, due to groundwater concerns. Large licensed buildings ("mausoleums") may be required to protect both materials and shapes. There is considerable usable equipment at the now-idle gaseous diffusion plant, K-25,

which cannot be used outside due to contamination with classified barrier material.

It should be noted, however, that this second option is probably only an interim measure, no matter how safe and secure the storage facility. Information with significant bearing on the environment, safety, and health in connection with DOE operations generally cannot, and should not, be kept classified.

Observation 3: ***The compositions and amounts of waste leaving DOE facility boundaries should be unclassified. Over the long term, all wastes not identifiable with specific weapons or tests should be unclassified.***

Production of Weapons Materials

Production of nuclear materials depends in part on classified technologies, e.g., uranium enrichment. Substantial declassification of such technologies would be inconsistent with nonproliferation policy. However, particularly under present conditions, declassification of total SNM (plutonium and enriched uranium) and tritium inventories and production rates would not appear to have significant national security impact. Such declassification would aid DOE in the preparation of completely unclassified environmental impact statements and might help improve the public image of the Department as supporting greater openness. Declassifications may also be necessary in order to comply with waste management regulations. As also discussed below in Section 5.3.5, the inventories reveal no information of proliferation concern.

Weapons Production, Assembly, and Disassembly

Weapons production, assembly, and disassembly lead to wastes and the waste management concerns described above. The public perceives that the degree of hazard depends on the amount of waste produced, and that this is roughly proportional to weapons production. While this is only approximately true, it raises the issue of whether weapon production rates should be declassified. This issue is discussed more fully in Section 5.3.5 below.

5.3.3 Technology Commercialization

DOE is making a strong effort to transfer technology developed in its programs, including classified nuclear programs, for application in the private sector, i.e., to "commercialize" such technology. Clearly, effective commercialization of classified technology will be difficult without a workable approach to accommodate both classification and commercialization concerns. The proposed commercialization of gaseous-diffusion barrier technology, now under review, provides an example involving currently classified uranium enrichment technology. An important lesson learned in this case is the need to bring in, at an early stage, all relevant expertise to assist in any declassification action; e.g., nonproliferation intelligence. (In this case, the initial declassification proposal was revised based on newly available information.)

Within the weapons design and development complex, there is little evidence that RD classification policy currently is having any substantial negative effect on DOE commercialization initiatives. One exception, voiced by several DOE laboratory spokesmen, may lie in what they view as excessive delays caused by classification review of technologies proposed for further development under Cooperative Research and Development Agreements (CRADAs). However, security measures (originating largely in the need to protect classified information) do impede access by uncleared industrial personnel to unclassified technologies that happen to be used in a secure environment. This presents a more severe problem for the DOE weapon production plants than for the weapon laboratories, and one that could impede commercialization efforts in the future, as the size of the overall program increases.

Cooperative research and development programs in which industrial personnel spend significant time on site must be carried out under security procedures appropriate for the work and for the DOE plant or laboratory environment. If the work itself is unclassified but must be carried out in an environment that is secure for other reasons, then the industrial personnel must be cleared. This greatly complicates and delays technology commercialization activities.

It is in the preliminary demonstration or "marketing" phase of technology commercialization that security procedures cause the most difficulties. The weapons laboratories have a great deal of experience in carrying out unclassified research programs, often in cooperation with industry or universities. Procedures established there can be readily adapted to allow controlled access to secure areas once all classified material has been removed or screened.

While the weapon production plants use little technology that is classified, their products generally are classified. Granting uncleared access to production lines to demonstrate manufacturing techniques currently requires that the line be shut down and all classified material removed or concealed from view.

On the whole, industry spokesmen in the area of technology commercialization do not seem too concerned about DOE classification policies. Some defense firms have worked with DOE laboratories on DOD-classified projects, and appear to be comfortable with their arrangements. One trade association spokesman asserted that while some of his members may be put off by a perception that DOE laboratories are too deeply involved with classified work to be worth approaching, none had raised this as a problem. Where there was any industry concern expressed, it always revolved around the plant access problems described earlier.

It should be noted that classified DOE technology can be transferred into industry for other <u>classified</u> defense applications with little difficulty. However, classified technology can be effectively commercialized only if the commercial application can be accomplished without classification restraints on the <u>product</u>, if not necessarily on the <u>process</u>. As with any classification question, deciding how to accomplish this will call for cost/risk/benefit analysis. No general rules can be established, since each case must be examined on its merits. This issue is most likely to occur with Special Nuclear Material (SNM) production technology, and perhaps weapons design computer codes and experimental techniques. For proposed commercialization objectives with technology related to gaseous diffusion barriers, for example,

declassification would be limited to information essential to the unclassified application. Membranes for commercial use might be manufactured using classified technology, but the barrier itself would not be classified.

From the above discussion, security -- not classification -- presents the primary obstacles to the demonstration and commercialization of unclassified technologies developed and used in classified programs at the DOE weapon plants and laboratories. Three options for dealing with this problem are:

- Build demonstration facilities outside security boundaries.

- Shut down operations and protect classified material prior to visits and demonstrations.

- Allow brief, incidental, partial access to classified materials to interim-cleared visitors.

The first option requires significant investment and potentially costly and wasteful duplication of facilities. The second results in increased operating costs and can impact performance schedules. The third option (perhaps modeled on the current pilot Accelerated Access Authorization (AAA) Program at Rocky Flats) would allow industry representatives to observe the production of classified parts without providing any further information. With only limited access, the observer would be unable to develop any comprehensive picture of classified technology. A check of government records (similar to current practice for clearance to the Secret NSI level) could be used for interim clearance to limit risk of any significant compromise.

The classification system must meet its overriding national security responsibilities but, where possible, it should facilitate and not impede technology commercialization.

Observation 4: ***Classification and security considerations should be addressed from the beginning of each technology commercialization project to help expedite the process while adequately protecting sensitive information.***

While this approach is already being implemented to a significant extent, it requires long-term emphasis. Other study observations and recommendations may also help in technology commercialization. Examples include the proposed major review of present classification to better define appropriate levels of sensitivity, broader participation in evaluating benefits and risks of declassification, and modified information security procedures.

At present, classification policy does not appear to be a substantial hindrance to DOE in its new mission of commercialization of technology developed for nuclear weapons and other classified applications. Most such technologies are themselves unclassified.

Observation 5: ***DOE field facilities need to plan and fund for better ways to address the security problem of access needed for outside people for technology demonstration and hands-on technology transfer. Possible ways to improve the access problem include short-term interim clearances, more flexible physical security arrangements, and demonstration facilities outside the fence.***

Commercialization of technologies that are still classified is a different problem. The benefits of commercialization have to be weighed against the risks of dissemination on a case-by-case basis. DOE should set up procedures to make sure that both benefits and risks are fully explored, with classification and security considerations addressed in a timely way. The process should involve the full range of relevant expertise on nuclear weapons technology and on likely commercial applications, with input from intelligence and from other agencies, as appropriate.

5.3.4 Modernization and Reconfiguration

Classification policy has an indirect effect on efforts to modernize and reconfigure the DOE Nuclear Weapons Complex. Classification -- or more accurately the security requirements stemming from the production of classified weapon parts -- was identified as slowing the introduction of new technology at Rocky Flats. This stems from the need to obtain Q-clearances

for the suppliers of the new technology, and from the long delays now characteristic of the clearance process. A pilot program to speed up this process, the Accelerated Access Authorization (AAA) Program is being tested at Rocky Flats.

DOE has goals for downsizing the weapons complex, standardizing much of the production, and reducing costs by obtaining non-nuclear components under competitive procurement from private industry. Planning for new and modified facilities should ensure that classification and security issues are addressed early in the design stage. Examples include greater attention to long-term costs for security, co-locating work of similar sensitivity, and planning for flexibility in physical security arrangements.

Classification and physical security could restrict DOE ability to use the most modern technologies in the private sector for use in the modernized weapons complex. Restricted access to facilities and the time required for obtaining security clearances of industrial personnel could be controlling factors in numerous decisions on technology. Pending a capability to grant clearances promptly, this problem should be addressed by instituting special programs to grant interim clearances (following credit checks and checks of other available files) and special limited access for individuals not having Q-clearances. The increased risk of disclosure of classified information could be minimal and would be greatly outweighed by full DOE access to the best available technology and industrial advice.

Reconfiguration plans include emphasis on standardization and on contracting-out production of non-nuclear parts of nuclear weapons to the private sector. For such "privatization" to lead to substantial savings, most of the work may need to be unclassified or at least have substantially reduced security costs. Major efforts are needed to explore the extent to which privatization can be done without undue risk to national security, while retaining substantial overall savings.

Observation 6: ***DOE should emphasize current efforts to reduce the operational penalties resulting from classification and associated security for new***

facilities by addressing them directly in the design stage, for example by co-locating classified work and allowing for adaptable security arrangements.

5.3.5 Nuclear Weapons Development

Throughout the DOE nuclear weapons complex it is frequently observed that there are too many classified documents, and that too many jobs require a Q-clearance. Both observations reflect the notion that too much material is classified, or classified too highly. However, a smaller number of people interviewed believe that in some areas too much information has already been declassified, with the U.S. by far the worst culprit when compared to other nuclear weapon states.

Weapons Research and Development

Many DOE laboratory staff members argue that classification policy has a direct and negative impact on their work by curtailing interactions with outside researchers. They argue that nuclear weapons R&D activities at the DOE laboratories are shrinking in size and that the laboratories no longer hold a monopoly on much of the scientific information and skills germane to weapons research. Continued progress requires improved linkage to the larger community found in universities and industry. This position is voiced very strongly, for example, by researchers in the inertial confinement fusion (ICF) program, by developers of computational physics codes, by scientists interested in the behavior of materials at extremely high energy densities, and by those interested in the properties and storage of hydrogen at high pressures. None of these fields is completely free of proliferation concerns.

ICF, for example, attempts to produce fusion energy from thermonuclear burn of small pellets of thermonuclear fuel, driven by powerful laser or charged particle beams. If successful, these small thermonuclear explosions could, in principle, be used for either military purposes (weapon physics, weapon-effects simulators, plutonium or tritium production) or civilian energy purposes (power reactors). ICF research is also useful for training people in the physics of high energy densities, basic to weapons technology. ICF

technology overlaps that of nuclear weapons, although there is little consensus on the degree or the importance of the overlap. ICF has been the most contentious and resource-consuming classification issue since the program began in the 1960s. There have been at least eight major reviews of ICF classification policy, including four within the last two years. The most recent study was made at the request of the Secretary of Energy to reconsider ICF classification policy in light of its potential as an energy source.

Declassification in areas such as weapons material science, computational physics, and ICF would allow closer collaboration between DOE researchers and outside scientists. In light of shrinking resources in the laboratories, closer coupling with the broader research community would probably speed progress and would make it easier for the laboratories to hire and retain good people. On the other hand, it is necessary to continue to examine the effect on U.S. nonproliferation interests of wider distribution of technology useful for development of advanced nuclear weapons.

In weapons science and computational physics, the end goal for the U.S. remains the improvement of the nuclear weapons technology base. In the case of ICF, the near-term goal is application to nuclear weapons science. However, the long-term goal is application to commercial power reactors and much of ICF technology relates to current weapons design more by analogy than by direct utility. In both areas, declassification would facilitate progress through improved domestic and international collaboration. However, the major U.S. effort in ICF and weapons science is centered in the DOE weapon laboratories, funded by the weapons program, and pursued in order to extend the boundaries of weapon science.

The common issue for classification of weapons science and ICF information is the implication for the proliferation of nuclear weapons, compared with the benefits of wider domestic and international participation. Opinions vary widely, with those in the ICF program strongly tending toward greater declassification, while people in the weapons program generally resist declassification on nonproliferation grounds. Classification policy is thus

particularly contentious in areas such as weapons science and ICF, which involve significant interests and capabilities outside DOE.

Observation 7: ***Special procedures need to be established for classification policy in areas such as weapons science and ICF, where significant interests and capabilities lie outside DOE, in order to ensure the fullest and most objective evaluation of both the risks and the benefits of declassification.***

These procedures might, for example, involve special carefully balanced panels of senior experts who are not directly involved in those programs to advise the Director of the Office of Security Affairs on major declassification actions.

Nuclear Testing

Many people interviewed said that it is no longer useful, or even possible, to classify the mere fact of nuclear tests at any substantial yield at the Nevada Test Site (NTS), or to classify their yield to within about 30%. They believe that there would be benefits from declassification of this information in the areas of arms control, operational efficiency, and particularly the credibility of the DOE classification system.

The present policy is to announce all current NTS events. Many but not all past events have been announced. Over 100 past event yields have been officially released, although only a very few recently. There is no apparent substantial benefit to potential adversaries or proliferators from release of this information.

Observation 8: ***The fact of all nuclear tests and their yields should be unclassified.***

Weapons Production

For the production plants, there are major programmatic costs to protect various associations of materials or combinations of materials with specific

plants, the weapons program, or specific weapons. For example, Y-12 has two major problems of this type. One is caused by requirements to protect the association of two materials with each other, although it is unclassified that both are, separately, associated with nuclear weapons. Another involves the association of a particular material (a natural choice) with a specific known function in nuclear weapons. Declassification could lead to substantial savings. As discussed earlier in connection with Environment, Safety, and Health, some of these classified associations may also conflict with legal requirements on future waste management.

The weapon production plants are often required to Q-clear essentially all workers by the terms of their labor contracts, which stipulate that work assignments should be readily reassignable. Where this is not the case, the plants can arrange classified production operations so as to reserve high level clearance and security procedures for only those facilities where it is absolutely necessary. However, some classification rules (e.g., regarding material associations) appear to lead to a higher level of security, and more paper work, than may be necessary under present conditions.

Plant personnel also noted inconsistencies between DOE and DOD classification policies that raise DOE production costs. As an example, in some cases DOE produces new weapons where the production rate and total build are classified, while DOD contractors produce entirely unclassified but similar numbers of corresponding system components. Since the programmatic costs of the higher DOE level of classification may be substantial, such apparent inconsistencies should be carefully examined. Where programmatic benefits can be clearly identified, declassification of production rates and inventories should be strongly considered.

Approximate values for the stockpile of some types of warheads (particularly strategic warheads) and for the total stockpile have long been widely available. It is not clear that either potential adversaries or proliferators would benefit from the U.S. revealing more data on inventories and annual production rates for nuclear weapons, or nuclear material. Making more detailed information available could conceivably make it more difficult to

protect sensitive nuclear weapon storage information on location, number, and type. However, on balance, there seems little reason for continued classification of most data on nuclear weapons production rates and stockpiles at this time.

Observation 9: ***Total inventories and annual production rates for nuclear materials (e.g., weapons-grade enriched uranium, plutonium, and tritium) and for nuclear weapons should be unclassified. (However, DOD may identify some of these data as militarily sensitive.)***

5.3.6 Information Security

This study primarily concerns classification, not security. Moreover, there has already been a major study on DOE security policy: "Report of the Secretary's Safeguards and Security Task Force," Major General James F. Freeze, USA (ret.), et al., December 1990, otherwise known as the "Freeze Report." Substantial changes in DOE security policy were recommended, many are now being implemented.

However, this study could not avoid some security issues since information security procedures are the principal way through which most people observe the effects of classification. The costs of classification to DOE internal operations are primarily the costs of maintaining additional security (over and above that needed to protect property) for the protection of classified information. There is an almost universal belief that there is too much material to protect since some of it is now unnecessarily classified, or too highly classified. As a result, overclassification interferes with the protection of truly sensitive information.

Classified information by nature of its origin falls into a number of distinct categories, e.g., information on nuclear weapons, military reactors, or isotope separation. Within each category, information is assigned levels of "Top Secret," "Secret," or "Confidential" according to its adjudged importance to national security. By definition, the unauthorized disclosure of any classified information could reasonably be expected to cause damage to the

national security. "Secret" information corresponds to "serious" damage and "Top Secret" to "exceptionally grave" damage to national security.

DOE now rarely uses Top Secret RD, at least in part because the information security requirements are felt to be too restrictive for practical use. While a good deal of nuclear weapons RD is classified Confidential, the bulk of weapons data appears to be classified at the Secret level. This is in distinct contrast to the practice of most other government agencies where both Top Secret (NSI) and Confidential (NSI) are used extensively.

However, information security procedures in other agencies for dealing with TS-NSI are more similar to those used by DOE for controlling access to Secret RD. DOD's information security treats Secret RD like Secret NSI, and so does not find the stricter S-RD accountability procedures specified for use within DOE a burden. (It should be noted that some of these DOE procedures have recently been relaxed.) Lack of common standards causes confusion, increases the risk of improper dissemination, and undermines the credibility of classification.

Access, Need-to-know

Overlaid on the classification system (which labels the level of sensitivity of information) and the personnel security system of individual clearances (certifying that access by that person to classified information would not damage national security) is a formalized system of "need-to-know" in which each classified program determines the required access of each individual to classified information in that area. RD weapons information access categories are labeled by Sigma categories, by the label of Weapons Data (now used primarily for formal reports, but currently under review), and by the designator "Critical Nuclear Weapon Design Information" (CNWDI) used by the DOD to control access of individuals holding NSI clearances to sensitive nuclear weapons design information (see definitions in Appendix F).

These various access categories have significant and confusing overlap and are no longer effective in controlling access to information. Therefore, to be

beneficial, any revision of classification policies should probably be coupled with a corresponding redefinition, and enforcement, of need-to-know procedures in each reasonably separable area of classified programs.

Observation 10: ***Need-to-know or access control criteria and procedures should be better defined and enforced, with appropriate compartments established to limit unnecessary dissemination of the most sensitive information.***

One especially troublesome combination of need-to-know and classification occurs in the category of information called "Sensitive Use Control Information" (SUCI). This is defined as information and hardware, knowledge of which would significantly enhance an adversary's ability to circumvent, or would permit circumvention of, nuclear weapon use control features. SUCI has been criticized on the grounds that:

- There is a lack of consistency in SUCI determinations. Laboratory program managers decide what is SUCI for their program without benefit of guidance. As a result, similar weapons can vary markedly in their SUCI content.

- Identification of parts as SUCI is controversial. Some production plants do identify parts while others argue that classifying a part as SRD provides adequate protection and do not label such parts as SUCI. They argue that marking SUCI parts would simply flag them for an insider adversary.

- Threat models and validated assessments of weapon use-control bypass scenarios are obviously very sensitive information, yet they are not classified as Top Secret because this makes the necessary accessibility too difficult.

The SUCI issue has recently been examined by the Technical Evaluation Panel, which recommended that bypass scenarios should be classified Top Secret and have very limited accessibility. Nuclear weapon parts involved in bypass scenarios should be classified because they are SUCI, but the hardware should

not be labeled as such. It appears that the issue of SUCI is now in the process of being dealt with appropriately, including definition of new Sigma categories.

Security Clearances

The excessive time required to process Q-clearances (currently a year or more) is a universal source of complaint. The weapon laboratories and plants generally require Q-clearance for anyone whose job entails regular access to the site, no matter what the chance that the job will allow effective access to classified material. Therefore, most janitors, painters, and similar support personnel receive Q-clearances. This seems to be more a matter of laboratory or plant policy than of DOE requirements, and undoubtedly is influenced by the fact that the full cost of clearances is not specifically identified by program or facility.

Personnel security and clearances were a principal concern of the Freeze Report. Clearances -- and particularly the time required to obtain them -- are a serious concern to most DOE operations. Major efforts are now being made to improve the security clearance process, including a successful pilot program at Rocky Flats to grant clearances locally, the Accelerated Access Authorization (AAA) Program.

Agency refusal to accept clearances or even background investigations from other agencies is widely recognized as a significant source of waste and delay, and is being addressed in the National Industrial Security Program (NISP) study. (NISP is a major Executive Branch effort to define government-wide standards for industrial security.)

An alternative that could be considered to partially relieve the congestion in the Q-clearance process would be to eliminate separate nuclear energy clearances entirely. If all departments of the Executive Branch operated with the same three clearance levels -- Confidential, Secret, and Top Secret (with perhaps the addition of the TS-Sensitive category for politically sensitive information) -- government and contractor operations would be greatly

simplified. Access to DOE information would still be controlled by need-to-know, in combination with the level of clearance specified. This works well today for Sensitive Compartmented Information (SCI); there appears to be no reason why RD could not be treated similarly.

Observation 11: ***A fundamental principle in any government information security system should be that the clearance and need-to-know requirements for access to any specific RD or NSI classified information should be the same throughout the government.***

Enforcement

Effective control of sensitive information through classification requires that the security system designed to protect classified information be enforced. Some legal authorities believe that the information control provisions of the AEA are vague, overly broad, and may be unconstitutional. This may lie behind the apparent reluctance of the Department of Justice (DOJ) to prosecute under the AEA. The DOJ seems to be less hesitant to deal with espionage, but most known infractions of the AEA do not appear to involve espionage. Instead, they generally take the form of leaks to the press to influence policy. There have been strong suggestions that DOE cannot expect to control such compromise of RD unless it:

- Makes sure its classification is credible.
- Establishes its own investigative authority and ability to enforce DOE regulations on its own personnel.
- Identifies and disciplines a few "leakers."

For each unauthorized disclosure of RD reported to DOJ for possible action, DOE must provide answers to a set of 11 questions before the DOJ will investigate. However, several of these questions would require preliminary investigation before they can be answered, and in many cases DOE feels it

lacks the needed authority. The general effect of this process is to discourage DOE efforts at enforcement.

While enforcement of DOE security controls on classified information is critically important, the subject is largely outside the scope of this study. However, based on comments during interviews, the issue of possible improvements in enforcement might involve:

- Reduction in the amount of classified information and documents to be protected.

- Maximizing public support of information security enforcement by better public description of the RD system and by wider participation in setting classification policy.

- Improvement in DOE internal enforcement of its orders and regulations, including a more effective system of investigation, administrative review, and penalties. Pre-employment agreements concerning review of future publications in classified areas might also help.

- Clarification of conditions under which the FBI will investigate possible violations.

- Removal of the present AEA requirements (in Chapter 18, "Enforcement") to establish "intent" or "reason to believe" (concerning injury to the United States or advantage to any other nation) for prosecuting knowing unauthorized possession or dissemination of RD.

Observation 12: ***Major efforts are needed to improve enforcement of the information control provisions of the Atomic Energy Act and DOE information security policy.***

Many of the earlier recommendations of this Classification Policy Study have implications for security policy. In particular, Recommendation 7 calls for a comprehensive fundamental review of current DOE classification policy guidance to better reflect current levels of sensitivity, including identifying the most sensitive information as Top Secret. As noted, use of Top Secret information would not be practical without changes in security procedures for Top Secret to make them more like current procedures for Secret RD.

Observation 13: ***DOE information security policy should be evaluated for changes which may be needed to implement the recommended changes in classification policy.***

5.3.7 The Costs of Classification

The fundamental criterion for classification in the AEA is that publication would cause "undue risk" to national security. Determining whether a risk is an "undue risk" implies a balancing between the risks and benefits of publication. The costs of classification are one factor which must be considered, although they are generally secondary except in comparing roughly equivalent levels of risk and benefit.

Identifying the costs of classification is a necessary preliminary to reducing them. The true costs of classification are difficult to determine. The most obvious dollar cost is for information security items such as clearances, guns, gates, guards, and safe files. However, the most significant "costs" of classification in some cases are the penalties to the classified programs and to other national objectives produced by the lack of free exchange of information. The costs of the resulting missed opportunities and inefficiencies are difficult to quantify but could be quite significant over the long term.

On occasion, costs associated with a classified program can be quite large, and identifiable. For example, the Air Force identified savings of about $80 million annually when it decided to declassify NASA shuttle flights with military R&D payloads. The avoided costs included documentation, control,

training, computer security, communications, entry systems, and payload logistics protection. The costs savings were so large because previously the Air Force was essentially installing its own security system in an otherwise unclassified NASA setting.

In the November 1990 report, The National Industrial Security Program: A Report to the President by the Secretary of Defense, estimates were presented for indirect impacts of government security requirements on security costs in private industry. For example, the National Industrial Security Program (NISP) report presents an estimate based on a survey of 14 companies by the Aerospace Industries Association (AIA) of about $44 million in salaries paid to employees awaiting clearances, alone. The total estimated costs of industrial security for the government-cleared facilities in the AIA survey amounted to $13.8 billion.

One of the conclusions of the report was that "the absence of a mechanism for determining complete and accurate costs makes it impossible to identify and forecast program expenditures or savings." The report recommended, as part of the future implementation plan, that a mechanism be established "for determining complete industrial security costs." These findings and recommendations for industrial security also have relevance for government security costs and (indirectly) for both government and contractor classification costs.

Increasingly limited budget resources and other major changes in national priorities make it important to estimate the costs of classification as well as possible. Reasonable cost estimates would be very useful for the major classification review called for by Recommendation 7.

DOE's Office of Safeguards and Security collects and analyzes information security and other security costs as part of the annual budget and planning process. Such information could provide a useful beginning for an improved assessment of the costs of DOE classification.

Observation 14: ***A formal process should be developed to estimate, as accurately as possible, the direct and indirect costs of classification and security policy.***

5.3.8 Implementation of Proposed Comprehensive Fundamental Review

Recommendation 7 calls for a comprehensive fundamental review of what nuclear weapon-related information should be protected under present circumstances. The expected future environment for classification was discussed above in Section 4.3. Particular issues and changed priorities in several areas were discussed in Sections 5.3.2 through 5.3.7, above.

Classification policy has extensively evolved over the past 45 years as evaluations of the balance between the risks and benefits of publication change. Pressures for declassification result from changes in foreign and domestic policy, as well as from economic and programmatic considerations. These must be balanced against the usually more slowly changing pressures for continued classification resulting from the fact that the risks associated with nuclear weapons continue to be grave and declassification is essentially irreversible.

Review Process

A fundamental review of what information on military uses of nuclear energy should be classified requires expert knowledge of the risks of publishing the technology, i.e., what information is both important to protect and can actually be protected in view of current worldwide capabilities. It also requires expert knowledge of the benefits of declassification to the nuclear weapons program or to other classified programs, to other areas of science or technology, and to economic (e.g., technology commercialization) or other national policy concerns such as international cooperation on control of nuclear weapons.

One possible way to bring this breadth of knowledge to bear would be for the Secretary of Energy to set up a high-level Review Group, perhaps based on the

Secretary of Energy's Advisory Board (SEAB). This Review Group would be asked to establish general criteria (some suggested criteria are given below) and specific recommendations for classification policy concerning what should be classified. The Review Group might find it useful to set up working groups in each major area of concern (e.g., nuclear weapons RD&T, production, and utilization; production of fissile material). Based on the Review Group's recommendations and comments from within DOE, DOD, and from the U.K., DOE would produce a revised DOE classification policy.

Implementation of New DOE Classification Policy

The Office of Classification would be responsible for implementing the new classification policy, with assistance from relevant Program Offices and representatives from the laboratories and production plants. There are likely to be substantial declassifications, changes in classification levels, and perhaps some limited reclassifications required.

A new revised hierarchy of classification guides would be needed. In particular, a new Classification Policy Guide needs to be developed giving general overall policy concerning what information still cannot be published without "undue risk" to national security. (It would be useful to have such a guide be unclassified.) Program Guides would then be revised as necessary to be consistent with the Policy Guide. Local Guides based on the Program Guides would be developed as needed. New guides will often require coordination with DOD and other agencies, and in some cases with the U.K.

Additional Institutional Changes

Additional efforts need to be made to keep classification policy and guidance current. There are existing requirements to review classification guides every two years. The process should be staggered to even out the load. Major reviews should be set for reasonable intervals, such as every 6 years, or whenever there are major changes in policy in that area.

The overall Classification Policy Guide should be periodically reviewed and revised as needed to reflect policy changes. In view of its role as a general policy statement, the guide would be more useful if it were changed to a narrative format from its current topical format.

DOE should also broaden its ongoing technical and policy advice to include the wider expertise required to evaluate both risks and benefits of declassification. For example, DOE's principal advisory body on technical classification policy, the Technical Evaluation Panel (TEP), should be broadened to include experts from outside the weapons laboratories, including the DOE production complex, the DOD, intelligence, foreign policy, industry, and the academic community. Similarly, the DOE classification system should make more use of a substantially broadened group of Responsible Reviewers, i.e., people with expertise in all of the technical areas involved who can provide classification advice as individuals, to complement the sometimes parochial programmatic and institutional views.

Suggested Criteria for Review

Suggested criteria for the recommended fundamental review are given below, in the form of a few general principles and some important considerations. A number of illustrative specific examples of information which might be appropriate for each level -- Top Secret, Secret, Confidential, and Unclassified -- follows the suggested criteria.

Principles and Important Considerations for a Comprehensive Review

The fundamental long-term objective of U.S. classification policy is to help protect national security and buy time for eventual international political solutions to the threat posed by nuclear weapons, including proliferation. It should be remembered that classification can help, but cannot do it all alone. Classification policy is only one of the tools used by the U.S. to protect nuclear weapons-related information. Information control, in turn, is only one of the aspects of overall U.S. national security policy in the areas of nuclear weapons and nonproliferation. Some general principles are:

- Classification policy should continue to require protection of information which would significantly help potential adversaries develop an initial nuclear weapons capability or improve existing weapons. It is also necessary to protect information in such areas as possible scenarios for unauthorized use of nuclear weapons, security information for nuclear facilities, and information potentially useful for developing countermeasures to U.S. nuclear weapons.

- The future effectiveness of U.S. classification policy for the control of nuclear weapons-related information requires a fundamental emphasis on international cooperation.

- Nuclear classification policy must take into account its effect on other U.S. national objectives such as environmental cleanup, technology commercialization, and cost reduction.

- Information control and classification policy must take into account the importance of both classified information and sensitive but unclassified information in restraining proliferation.

More specific considerations for classification determination should include:

- The extent to which the information would assist potential adversaries in the development of an initial nuclear weapon capability or in improvements to existing nuclear weapons.

- The extent to which the information would assist others in countermeasures against U.S. nuclear weapons, or in unauthorized use.

- The extent to which the information would assist in the production of special nuclear material (if applicable).

- The cost in terms of time and money of acquiring the information independently.

- The state of the art for the information in both the U.S. and in other countries.

- The benefit to U.S. public welfare from the declassification, including improvements in environment, safety, and health and any significant technology commercialization potential.

- Any detrimental (or beneficial) effect that release of the information might have on U.S. foreign relations, arms control negotiations, or treaty obligations.

- Any impact on the credibility and effectiveness of the Department of Energy classification program caused by the continued classification of the information.

- Any penalties to U.S. programs due to the continued classification of the information.

Illustrative Examples

Illustrative examples for each level of classification are given below which are generally consistent with the preceding criteria. Of course, specific items within these categories may be assigned different levels of classification by the proposed fundamental review. Other items related to military utilization may have additional sensitivity for DOD.

- Most Sensitive (Top Secret)

  This level of sensitivity refers to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. It should include technical information of a specific and comprehensive nature

describing nuclear explosive designs or operational sensitivities. Suggested candidates include:

- Complete designs (drawings, design reports, etc.) of nuclear weapons or nuclear explosive devices
- Weapon design handbooks, compilations
- Significant vulnerabilities of U.S. weapons
- Validated assessments and threat definitions for unauthorized use of nuclear weapons, or access to Category I amounts of special nuclear material

NOTE: These suggested changes would greatly expand the use of TS-RD. For use of the level Top Secret to be practical, appropriate changes must be made in DOE information security procedures to make them more practical and comparable to those in other agencies.

- Sensitive (Secret)

This level of sensitivity should include technical information (general or specific) whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security, but that is not so comprehensive as to reveal a complete device design or a significant vulnerability. Suggested candidates include:

- Component designs and drawings
- Manufacturing specifications
- Weapon design computer codes (so identified)
- Nuclear test reports
- Material properties (e.g., opacities, equations of state) of weapons materials in the range of interest for weapon design
- Complete design or key features of uranium and plutonium isotope separation technologies

- Less Sensitive (Confidential)

  Unauthorized disclosure of confidential information could reasonably be expected to cause damage to the national security. This level of sensitivity should include information of less sensitivity than TS or S, but deemed to be of significant use to an adversary or proliferator, and not readily deducible by competent professionals from general physical principles or from information already in the public domain. Suggested candidates include:

  - Design of firing sets and safing systems
  - Number of detonators in a nuclear weapon
  - Inertial confinement fusion technology (most remaining classified aspects)

- No Longer Sensitive (Declassified)

  This category should include nuclear-related technical information whose unauthorized disclosure could, on balance, reasonably be expected to cause no damage to the national security. Suggested candidates for declassification include:

  - Waste leaving DOE facilities
  - Certain mere associations between materials and weapons production facilities, or weapons (specified or unspecified)
  - Compositions, inventories, and annual production rates of many weapons materials
  - Fact of all nuclear tests and their yields
  - Inventories and annual production rates of nuclear weapons (Note that DOD may identify some such data as militarily sensitive.)

6. GENERAL CONCLUSIONS

In the course of this study, several alternative classification systems to the current Restricted Data (RD) system were analyzed and evaluated. After considering the advantages and disadvantages of each alternative, it was concluded that the present RD system should be retained but with major legislative and non-legislative changes designed to improve the effectiveness of the system in a rapidly changing world.

The recommended changes are needed to increase the flexibility, credibility and comparability of the RD system. The increased flexibility will permit international cooperation with other countries through the limited exchange of RD as needed to control proliferation, improve nuclear weapon safety, verify treaty compliance, assist in the dismantlement of foreign nuclear weapons, and for other purposes. The Atomic Energy Act now contains provisions that strictly limit the exchange of nuclear weapons information so that legislative changes would be needed to obtain the needed flexibility.

The credibility of the RD system can be increased through a fundamental review of all information concerning nuclear weapons-related technology. The objective of such a review would be to remove from classification any information that careful analysis of current benefits and risks shows could be published without "undue risk" to national security. The review would be responsive to the comments of a significant number of the people interviewed during the course of the study who believe that there is too much overclassification of information within DOE. The recommendations for eliminating "private Restricted Data" and for clarification of controls on sensitive unclassified information would also improve credibility.

Most users of RD are also users of NSI. Comparability of operational procedures is desirable to minimize the risks of confusion, and costs. In view of the close interaction between classification and security, the existing information security policy should be examined to identify those changes needed to implement the recommendations affecting classification policy. These changes, together with the legislative and non-legislative

changes recommended, would increase the operational comparability between the RD system and the NSI system and would support the principle that the requirements for access to and protection of a specific piece of classified information should be uniform throughout the government.

The recommendations of this study represent only a beginning for constructive modification of the RD system. Some of these suggested modifications will require considerable additional input from DOE Program Offices, other agencies, Congress, other concerned institutions, the U.K., and perhaps other countries. Implementation of the recommendations will require a detailed coordinated program for proposed legislative changes and specific administrative, programmatic, and policy guidance. The fundamental review of all nuclear weapons information will require a large-scale commitment by the DOE classification community. However, the opportunities for an increase in the flexibility, credibility and comparability of the DOE classification system argue strongly for implementing the recommended changes.

6.1 Summary of Observations

This section gives a summary list of the observations made in this study.

Observation 1: *High priority should be given to efforts to arrive at common international standards for classification and other controls on nuclear weapons-related technology* (p. 52).

Observation 2: *Specific legislative authority is needed for DOE to withhold Export Controlled Information (ECI) from release under the Freedom of Information Act. In addition, formal procedures need to be established for a DOE-wide "Official Use Only" (OUO) Information Program* (p. 68).

Observation 3: *The compositions and amounts of waste leaving DOE facility boundaries should be unclassified. Over the long term, all wastes not identifiable with specific weapons or tests should be unclassified* (p. 76).

Observation 4: *Classification and security considerations should be addressed from the beginning of each technology commercialization project to help expedite the process while adequately protecting sensitive information* (p. 79).

Observation 5: *DOE field facilities need to plan and fund for better ways to address the security problem of access needed for outside people for technology demonstration and hands-on technology transfer. Possible ways to improve the access problem include short-term interim clearances, more flexible physical security arrangements, and demonstration facilities outside the fence* (p. 80).

Observation 6: *DOE should emphasize current efforts to reduce the operational penalties resulting from classification and associated security for new facilities by addressing them directly in the design stage, for example by co-locating classified work and allowing for adaptable security arrangements* (p. 81).

Observation 7: *Special procedures need to be established for classification policy in areas such as weapons science and ICF, where significant interests and capabilities lie outside DOE, in order to ensure the fullest and most objective evaluation of both the risks and the benefits of declassification* (p. 84).

Observation 8: *The fact of all nuclear tests and their yields should be unclassified* (p. 84).

Observation 9: *Total inventories and annual production rates for nuclear materials (e.g., weapons-grade enriched uranium, plutonium, and tritium) and for nuclear weapons should be unclassified. (However, DOD may identify some of these data as militarily sensitive)* (p. 86).

Observation 10: *Need-to-know or access control criteria and procedures should be better defined and enforced, with appropriate compartments established to limit unnecessary dissemination of the most sensitive information* (p. 88).

Observation 11: *A fundamental principle in any government information security system should be that the clearance and need-to-know requirements for access to any specific RD or NSI classified information should be the same throughout the government* (p. 90).

Observation 12: *Major efforts are needed to improve enforcement of the information control provisions of the Atomic Energy Act and DOE information security policy* (p. 91).

Observation 13: *DOE information security policy should be evaluated for changes which may be needed to implement the recommended changes in classification policy* (p. 92).

Observation 14: *A formal process should be developed to estimate, as accurately as possible, the direct and indirect costs of classification and security policy* (p. 94).

6.2 SUMMARY OF RECOMMENDATIONS

This section gives a summary list of the recommendations of the study from Section 5.

- **Recommendation 1**: Retain the current Restricted Data system, but with appropriate structural modifications (p. 48).

- **Recommendation 2**: Amend the Atomic Energy Act to allow the Secretary of Energy, in coordination with appropriate executive and legislative branch authorities, to approve communication of carefully limited Restricted Data to selected nations for the purposes of more effective cooperation on arms control, nonproliferation, combating nuclear terrorism, and nuclear weapon safety (p. 53).

- **Recommendation 3**: Amend the Atomic Energy Act to eliminate the Formerly Restricted Data (FRD) category now used to identify military utilization information and transfer such information to NSI (p. 56).

- **Recommendation 4**: Amend the Atomic Energy Act to allow the Secretary of Energy under carefully prescribed conditions to reclassify specific information in areas of Restricted Data that have previously been declassified (p. 58).

- **Recommendation 5**: Amend the Atomic Energy Act to eliminate privately generated information from the definition of Restricted Data (p. 61).

- **Recommendation 6:** Amend the Atomic Energy Act to better define the scope and enforceability of Unclassified Controlled Nuclear Information (UCNI) (p. 66).

- **Recommendation 7:** Conduct a comprehensive, fundamental review of all nuclear weapon-related information to determine what should be classified under present conditions, with the objective of removing from classification all information that no longer warrants such protection (p. 71).

7. APPENDICES

memorandum

DATE: MAR 2 4 1990

REPLY TO ATTN OF: DP-32

SUBJECT: Defense Programs' Classification Policy Study

TO: Distribution

Defense Programs (DP) is undertaking a comprehensive classification policy study to determine whether continuation of the present Department of Energy (DOE) classification policies and procedures will remain adequate and appropriate for the coming decade ahead and beyond.

The world situation is vastly different than the one that existed in 1947 when the Atomic Energy Act became effective. The U.S. nuclear monopoly has long since ended. There has been a significant impact on our economic posture as a result of increased world-wide competitiveness. The cold war seems to be on the verge of ending. Arms control negotiations have brought an Intermediate Nuclear Forces (INF) Agreement with the prospect of others to follow. The Department, in turn, is continuing to face new challenges and goals: an initiative for effectively commercializing technology developed in DP's laboratories to enhance U.S. economic competitiveness, a comprehensive environmental restoration program, a major plan for modernization of the nuclear weapons complex, etc. All these and other factors argue for a fresh look at our DOE classification program to ensure that our policies and procedures are in step with the new national and international environment and the role that the Department will play.

As for the study, it is our plan to have a Working Group that will be responsible for performing the various detailed tasks associated with the study (e.g., research, interviews, etc.) and the writing of the final report. This group will operate under the direction of the Office of Classification and Technology Policy (DP-32) and will be comprised of a few senior individuals with extensive experience in the national and international security aspects of DP. Dr. Ray Pollock will be the Director of the Working Group and assisting him will be Dr. William Grayson and Mr. John Griffin.

In addition to the Working Group, we also plan to have a review group that would be comprised of senior people of recognized national stature. This group will review the study results and provide an evaluation of the significance for U.S. national security policy. The actual membership of the group will be determined at a later date.

An outline of the study has been prepared, and I have attached a copy for your information. Please provide any comments you might have on the outline to DP-32. I ask for your cooperation and that of your

staff in responding to requests by members of the Working Group for interviews or other information. I think it is very important that we have the benefit of your views on the direction of the DOE classification program for the future.

I plan to keep you advised on the progress of the study through periodic status reports. Your cooperation is greatly appreciated.

John C. Tuck
Under Secretary

Attachment

CLASSIFICATION POLICY STUDY

PURPOSE

To determine whether continuation of present Department of Energy (DOE) classification policies and procedures will remain adequate and appropriate for the future.

SCOPE

This study will examine the function and effects of the present Restricted Data (RD) system of classification in order to gauge its suitability for the future. While this will include a review of past effectiveness, the principal purpose will be to identify and assess the benefits and costs of classification in the current and anticipated future-world environments.

BACKGROUND/DISCUSSION

The U.S. Government classifies material relating to the design, production, and utilization of nuclear weapons in order to deny an enemy access to information that could compromise the effectiveness of U.S. weapons systems and to hamper progress of would-be nuclear proliferators. However, classification can have negative impacts: loss of public confidence if classification appears misused or excessive; economic costs from lost commercial opportunities; "stiffening" of the research and development process that can add to costs and impede technology transfer; and complications in U.S./allied military planning and operations.

While much military- or defense-related information is classified by executive order as National Security Information (NSI), the classification of RD applied to nuclear-weapons data is unique in that it is established by statute in the Atomic Energy Act. The Act mandates that all information falling within the definition of RD is born classified and can be declassified only by specific action. In contrast, the NSI system reverses the procedure and requires a specific determination to classify.

This review will focus on the effects of present policies and any proposed changes. Questions appropriate for examination include:

- Are U.S./USSR arms control agreements likely to lead to pressures to liberalize the DOE classification policies or to find other ways to exclusively share with the USSR information presently classified as RD, e.g., safety features of weapons?

- Is present policy adequate to deal with current and future anticipated proliferation threats?

- Is classification as RD an impediment to joint efforts by nuclear powers to counter terrorism and proliferation?

- o Would wider international cooperation on classification policies be in the national interest?

- o Are the benefits of the present classification system commensurate with the costs imposed and are they likely to remain so?

  - Has the system contributed to perceived DOE indifference to the public interest and environmental, safety, and health concerns?

  - Does classification as RD provide particular impediments to research and development, technology transfer, and technology commercialization?

  - How does the advent of electronic data processing with worldwide access impact the cost of classification?

  - Is the distinction between RD and NSI being well maintained throughout the defense community? Does it remain a useful distinction?

  - How does the increasing number of technical conferences world wide with scientists exchanging information impact classification?

  - Would military operations of the United States and its allies benefit if information now classified as Formerly Restricted Data (FRD) were transclassified to NSI?

  - Do classification policies that affect technology transfer need to be changed to foster U.S. economic competitiveness?

- o Does the principle of "born classified" remain useful, given the wide availability of nuclear information? If this were to be abandoned, would the ability to administratively establish classification boundaries and durations as the situation demanded, including the option to reclassify some previously declassified RD as NSI, be useful to national security?

- o Would amendment of the Atomic Energy Act to preserve the category of RD but leave it to the Executive Branch to define the information included therein be a useful alternative?

PROCEDURE

The study will be broken into four tasks as described below. Only a relatively small portion of this work can be based on established fact and record. Most of the effort must go into solicitation of informed opinion and expert judgement resident in the national laboratories, military services, industry, and Government. This will be accomplished through direct interviews, questionnaires, and the preparation of issue papers for review and comment.

Task 1. Determine historical effectiveness of the present system of classification.

Previous laboratory work, public documents, and the Office of Classification and Technology Policy records will be reviewed and case histories analyzed to determine the extent to which nuclear weapons information has reached the public by other than official declassification actions. The possibility that information has remained classified beyond the time when it represented an undue risk to the common defense and security will also be examined.

Task 2. Project the likely future environment within which the DOE classification system must function.

The future international security environment will be projected by reviewing the Bush Administration's national security studies and other recent work. Expectations for the role of classification policy in the future nonproliferation regime will receive particular attention. Potential U.S./USSR arms control agreements will be analyzed to determine any consequences verification considerations may hold for classification requirements. The value of continued classification of information relating to DOE operations (stockpile size, production rates, requirements, and technologies) in a domestic environment characterized by increased emphasis on technology to support U.S. competitiveness, and growing concern for the environment, will be examined.

Task 3. Evaluate certain costs and benefits of classification and examine the utility of preserving the distinction between RD and NSI.

By examining DOE classification guidance, the extent to which "born classified" has swept up "nuclear-irrelevant" information, i.e., information in areas such as laser technology or pulsed power, only marginally related to nuclear weapons, will be determined. The importance of such information will be assessed as part of a broader examination into just how classification affects efforts to transfer DOE technology to industry. Case studies of specific research and development enterprises--for example, inertial confinement fusion or uranium enrichment--will be undertaken to attempt to illuminate the tensions between classification and commercialization policies.

Similarly, the merits and disadvantages of abandoning the FRD classification for military/operational information in favor of broader use of the NSI category will be reviewed.

In summary, in this principal task the costs and benefits of existing classification policy and the RD/NSI distinction will be identified and presented. The ramifications of elimination of RD as a category of classified information will be examined.

Task 4. In light of the conclusions of Tasks 1 through 3, develop any proposals for change and package the study for presentation to the review group.

A report will be prepared detailing how well the present system has worked, what its costs have been, and the problems it may encounter in the future. Suggestions for improvement and policy alternatives will be developed and the impact of carrying out any of these proposed actions evaluated.

APPENDIX B

History of Classification: RD and NSI

B.1 Restricted Data (RD)

Introduction

With the approval by President Roosevelt in October 1939 of uranium research (based in part on Albert Einstein's letter alerting him to the possibility of building "extremely powerful bombs" using uranium), the first of many decisions had been made that would lead to the Manhattan Project and the successful U.S. effort to build an atomic bomb. While the early stages of the U.S. effort had been dominated by research scientists, the establishment of the Manhattan Engineering District in August 1942 under the U.S. Army Corps of Engineers placed the scientists effectively in a supporting role in the construction phase of a very large, high priority project run by the military. Colonel Groves (soon to be promoted to Brigadier General) was appointed to head the Manhattan Project.

The Manhattan Project

The Manhattan Project was carried out under a mantle of military security where essentially all information was classified. The secrecy and compartmentalization of information surrounding the Manhattan Project was a constant irritant to many of those working on it, who considered it a major impediment to success (though perhaps necessary under the circumstances). After the surrender of Japan in 1945 pressure began to build for the declassification of various aspects of the project.

Anticipating the need to provide information on the Manhattan Project once the devastating power of the atomic bomb had been demonstrated, Dr. Henry Smyth was assigned the task in March 1944 to begin work on a technical history of the wartime program, but within the constraints of carefully drawn guidelines. It was believed that such a technical report would provide a basis for rational public discussion while helping to protect the essential military secrets. However, there were major misgivings and opposition within the U.S. Government to the release of such a full description.

After the report had been completed, the matter of review and clearance within the U.S. Government began. While there continued to be opposition to publishing the report within the U.S., the strongest opposition to publication came from the British. However, the report was cleared for immediate release by President Truman on August 9, 1945 the same day that the second bomb was dropped on Nagasaki. Sunday morning newspapers of August 12 carried excerpts from the report, two days before the Japanese surrender on August 14. While the Smyth report: "A General Account of the Development of Methods of Using Atomic Energy for Military Purposes under the Auspices of the United States Government, 1940 - 45", H. D. Smyth, USGPO, Washington, (August 1945) was the first detailed information on the wartime program, the veil of secrecy was

originally lifted by President Truman's statement following the atomic bomb attack on Hiroshima on August 6.

The Tolman Committee

Early in November 1945, in response to an avalanche of requests from scientists and contractors to declassify their wartime research and development in atomic energy, General Groves asked Dr. Richard Tolman to develop a declassification policy for the great volume of classified information that had been generated during the Manhattan Project. A committee including Robert Bacher, Ernest Lawrence, Robert Oppenheimer, Frank Spedding, Harold Urey, and Tolman met in November 1945 to develop a general policy regarding the release of scientific and technical information developed during the project. The committee developed a topical list of research and production activities in the Manhattan Project and placed each subject in one of three categories:

- Category I - Information recommended for immediate declassification
- Category II - Information whose declassification would be conducive to the national welfare and to long term national security.
- Category III - Information not recommended for declassification

The Tolman Committee report was cleared by General Groves and President Truman and the declassification policy contained in the report was published in March 1946 as the "Declassification Guide for Responsible Reviewers."

The committee also proposed forming a group of responsible reviewers, senior technical experts in relevant fields, who would consider documents for declassification. The first four Senior Responsible Reviewers appointed were: Warren Johnson for the pile project; Willard Libby for gaseous diffusion; Robert Thornton for electromagnetic separation, and John Manley for weapons. The Senior Responsible Reviewers declassified about 500 documents before the end of 1946 which, although dismissed by outside scientists as insignificant, represented a considerable effort. The Senior Responsible Reviewers evolved into a standing "Committee of Senior Reviewers" which served as principal advisors to the Atomic Energy Commission on classification matters until superseded by the current group, the Technical Evaluation Panel (TEP), in 1978.

It is worth noting that when the first declassification guide was published in March 1946 there was no Atomic Energy Act, no Atomic Energy Commission, and no category of classified information known as Restricted Data. However, the work of the Tolman Committee and the classification system of the Manhattan Project formed the basis for the classification program of the Atomic Energy Commission when it came into existence in January 1947.

The Atomic Energy Act of 1946

The early thinking on a statute to control the devastating power of the atomic bomb started well before the use of the bomb on Japan. There was much activity within the Executive Branch in drafting legislation that led to a bill which was introduced in the Congress in October 1945. However, there were provisions in the proposed legislation that triggered opposition from the scientific community and others both within and outside the government.

The legislative battle to pass the Atomic Energy Act stretched over a period from October 1945 until July 1946. While there were a number of contentious issues debated, the overriding one was civilian versus military control of atomic energy. There was also much controversy over Section 10 which at one point was titled "Dissemination of Information" but was later changed to "Control of Information." Section 10 in the 1946 act contained the definition of Restricted Data (RD) that read:

> The term "restricted data" as used in this section means all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security.

Although RD was not specifically referred to in the 1946 act as "classified" information, an FBI investigation was required for a person to have access to it. Also, the Act did provide authority for the Commission to remove information from the RD category (i.e., declassify it) provided it could be published without adversely affecting the common defense and security.

Whereas the 1946 Act contained no provisions for the communication of RD to any other nation, a 1951 amendment did provide for the communication of RD (other than weapons information) to another country under certain conditions and with the approval of the President and the consent of the Congress.

The Atomic Energy Act of 1954

A major revision of the Atomic Energy Act occurred in 1954 that resulted in several significant changes related to the handling and dissemination of RD*. The changes that affected classification were consistent with other changes in the 1954 Act that were designed to make some selected atomic energy information more accessible to the U.S. military, to U.S. industry and to the rest of the world. This objective was also reflected in President Eisenhower's Atoms for Peace initiatives which were included in his 1953 speech to the United Nations. These initiatives were directed toward developing the industrial applications of atomic energy.

---

*See Appendix D for relevant excerpts.

The 1954 Act contained the following provisions that related to the classification, declassification, and dissemination of RD:

- Section 142 was added under Chapter 12 "Control of Information" (formerly Chapter 10 of the AEA of 1946) - and was titled "Classification and Declassification of Restricted Data" and contained the following authority:

  Sec. 142, Classification and Declassification of Restricted Data.-

  a. The Commission* shall from time to time determine the data within the definition of Restricted Data, which can be published without undue risk to the common defense and security and shall thereupon cause such data to be declassified and removed from the category of Restricted Data.

  b. The Commission shall maintain a continuous review of Restricted Data and of any Classification Guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data which have been declassified in order to determine which information may be declassified and removed from the category of Restricted Data without undue risk to the common defense and security.

  c. In the case of Restricted Data which the Commission and the Department of Defense jointly determine to relate primarily to the military utilization of atomic weapons, the determination that such data may be published without constituting an unreasonable risk to the common defense and security shall be made by the Commission and the Department of Defense jointly, and if the Commission and the Department of Defense do not agree, the determination shall be made by the President.

  d. The Commission shall remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and Department of Defense jointly determine can be adequately safeguarded as defense information: *Provided, however*, That no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with subsection 144 b.

---

*"Commission" should now be read as the "Secretary of Energy."

e. The Commission shall remove from the Restricted Data category such information concerning the atomic energy programs of other nations as the Commission and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 102(d) of the National Security Act of 1947, as amended, and can be adequately safeguarded as defense information.

- Added the word "design" to the definition of RD so that it now reads "design, manufacture, or utilization of atomic weapons."

- Added Section 144 - "International Cooperation" - that provides for dissemination of RD to other nations under certain specified conditions. This provision was a further extension of the authority in the 1951 amendment since Section 144 includes dissemination of atomic weapon information, a category that was expressly prohibited in the 1951 Amendment.

The provisions of the 1954 Act that affect classification and dissemination of RD information remain essentially unchanged, and represent the legal foundation on which the current DOE RD classification system is based.

Over the years much information which was once RD has been declassified, largely to facilitate commercial applications. Complete program areas such as civil power reactors and nuclear fuel reprocessing have been removed from the RD category through declassification. Whereas essentially all atomic energy information was classified in the early days, there are relatively few remaining areas of national defense - related classified RD:

- Nuclear weapon design
- Nuclear material and nuclear weapon production
- Inertial confinement fusion
- Military reactors
- Isotope separation
- Directed nuclear energy systems

There are certain unique features of RD that distinguish it from other classified information, in addition to its statutory basis. RD is generally technical rather than policy or operational information. It does not take a specific act by an authorized person to classify RD. Information that falls within the definition of RD is classified when it is originated; i.e., it is "born classified". National Security Information (NSI), on the other hand, is essentially "born unclassified" (except for foreign government information and certain intelligence information) and it takes an action by an authorized person to determine that it is classified. RD information can be declassified only if it meets the criterion contained in the Act (i.e., that it may be published without undue risk to national security), and only by a person specifically delegated this function by the Secretary of Energy (now the Director of the Office of Security Affairs).

Another unique feature of RD is that it applies not only to information owned or controlled by the government but also to "all" information falling within the RD definition, including that originated in the private sector, hence the term "private Restricted Data." While this provision of the Act has been subject to controversy, it has been applied successfully in a number of cases.

The act also provides for removing information primarily related to military utilization from RD and putting it under joint control of the DOD and DOE, to be treated as NSI domestically but remain subject to a formal Agreement for Cooperation for international dissemination. This category of information is known as "Formerly Restricted Data (FRD)." In addition, foreign intelligence information of an RD character may be transclassified to NSI by the joint action of the Director of Central Intelligence and DOE.

The RD classification system differs in a number of fundamental ways from NSI which is classified under Executive Order 12356. NSI is discussed in more detail in the next section.

B.2 National Security Information (NSI)

Introduction

National Security Information (NSI) is the present name for government information whose unauthorized disclosure could reasonably be expected to cause damage to the national security (both RD and FRD are excluded).*

Executive Order 8381 (March 1940) - The First Order

While the classification of military information dates back as far as the earliest days of our country, the origins of the present national security classification system can be traced to just prior to World War I. The first use of an Executive Order for security classification took place when President Roosevelt issued Executive Order 8381 in March 1940, entitled "Defining Certain Vital Military and Naval Installations and Equipment." As authority, he cited the Act of January 12, 1938 (Public Law 418, 75th Cong., 52 Stat. 3), which stated:

> Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installation or equipment without first obtaining permission of the commanding officer.

Violation of the law was subject to criminal action, a $1,000 fine and/or imprisonment of up to 1 year.

This order was general in nature and relatively brief (about 1 page) when compared to Executive Order 12356** (12 pages) that is in effect at the present time. Although it referred to the classification terms "Secret," "Confidential," and "Restricted," it did not define them.

A government-wide regulation dealing with security classification was issued in September 1942 by the Office of War Information (OWI) which provided definitions of the three categories of classified information contained in the Executive Order, as follows:

---

*An important source of information concerning classification is "Security Classification of Information," Oak Ridge Gaseous Diffusion Plant K/CG-1077, V1, Arvin S. Quist, (September 1989)

**See Appendix E

Secret Information is information the disclosure of which might endanger national security, or cause serious injury to the Nation or any governmental activity thereof.

Confidential Information is information the disclosure of which although not endangering the national security would impair the effectiveness of governmental activity in the prosecution of the war.

Restricted Information is information the disclosure of which should be limited for reasons of administrative privacy, or is information not classified as confidential because the benefits to be gained by a lower classification, such as permitting wider dissemination where necessary to effect the expeditious accomplishment of a particular project, outweigh the value of the additional security obtainable from the higher classification.

Executive Order 10104 (February 1950) - A Continued Policy

Ten years after the issuance of Executive Order 8381, President Truman issued Executive Order 10104, "Definition of Vital Military and Naval Installations and Equipment" in February 1950 using the same statutory authority as the preceding order and also "in the interest of national defense." This new order continued authorization for the classification markings of Secret, Confidential, and Restricted and formalized the designation Top Secret. Top Secret was already in use and had been added to military regulations to correspond to the classification levels of our allies in the latter part of World War I. This order was also brief and did not define the terms Top Secret, Secret, Confidential, and Restricted. Even though the Atomic Energy Act was in existence at the time, the order made no reference to the Act or to Restricted Data.

Executive Order 10290 (September 1951) - A Broadened Classification System

The following year in September 1951, President Truman issued Executive Order 10290 that formalized and extended the security classification system to non-military agencies as well as the Defense Establishment. The authority cited in this order was "the Constitution and statutes and as President of the United States." The order permitted any executive department to classify information and defined "Classified Security Information" as "official information the safeguarding of which is necessary in the interest of national security, and which is classified for such purposes by appropriate classifying authority." This order was very detailed and similar in content to the current Executive Order 12356. Although containing a definition section, it did not define the terms Top Secret, Secret, Confidential, and Restricted, but did include criteria to be used in determining the use of these classification markings. It also contained several sections including those dealing with declassification and downgrading, dissemination, and security procedures. It was the first Executive Order to acknowledge and define Restricted Data (RD) and to exempt RD from its provisions, as did all subsequent orders.

While the order was criticized by some segments of the press because of its vagueness and potential for abuse, it did set the pattern for subsequent orders in both content and format.

Executive Order 10501 (November 1953) - A Change in Direction

President Eisenhower, responding in part to the criticism of Executive Order 10290, issued Executive Order 10501 in November 1953 which significantly reduced the number of agencies authorized to classify information, eliminated the Restricted category, and redefined the use of the three authorized classification markings. It eliminated classification authority for 28 government agencies and limited the authority of 17 others to the head of the agency. This was the first order that provided examples of the types of information that could be classified as Top Secret and Secret. It was of interest that "scientific and technological developments" vital or important to the national defense could be so classified. The press release accompanying the order emphasized that it was designed to attain the proper balance between the need to protect information important to the defense of the United States and the need for citizens to know what their government is doing. The authority for this order was "the authority vested in me by the Constitution and statutes, and as a President of the United States."

Whereas Executive Order 10290 was perceived as relaxing the requirements to classify information, this order changed the direction of the classification system toward a much more disciplined regime. With the issuance of new Executive Orders by succeeding presidential administrations, one could observe either the perceived relaxation or tightening of the government's classification rules.

Although Executive Order 10501 was modified from time to time, it served as the classification authority until it was superseded in June 1972.

Executive Order 11652 (March 1972) - Some New Innovations

In January 1971, President Nixon directed an interagency review of the security classification system with the objective of proposing steps that might be taken to provide for more rapid declassification. The review was undertaken, in part, because of the "Pentagon Papers" episode. The Chairman of the interagency committee was William H. Rehnquist, an Assistant Attorney General until his appointment to the Supreme Court in late 1971. The product of the interagency group was Executive Order 11652 which was issued in March 1972 with effective date of June 1, 1972. The authority for this order was "the Constitution and statutes of the United States."

Executive Order 11652 incorporated several new provisions as follows:

- Reduced substantially the number of departments and people who could originally classify information.

- Established timetables from 6 to 10 years for the automatic declassification of documents, with exemptions permitted.

- Established a mandatory review procedure based upon a request from a private citizen for documents exempted from the automatic declassification provisions and that had been classified for 10 years.

- Established automatic declassification for documents over 30 years old unless exempted in writing by the head of the originating department.

- Incorporated prohibition of classification to conceal inefficiency or administrative error or to prevent embarrassment to a person or Department.

- Expanded classification training and orientation programs.

- Established an implementation and monitoring process set up under the National Security Council and the Interagency Classification Review Committee. The committee consisted of members from the Departments of State, Defense, and Justice; the Central Intelligence Agency; the Atomic Energy Commission; and the NSC staff. The President designated the Archivist of the United States as Chairman.

At about this same time, the Foreign Operations and Government Information Subcommittee of the House Committee on Government Operations was holding hearings on the government classification system as it had operated under Presidential Executive Orders. A conclusion contained in the Subcommittee's report of the hearings was that a statutory classification system should be established to make it clear that Congress intends a proper balancing between the safeguarding of information classified under strict guidelines to protect vital defense and foreign policy secrets and the right of the public to know about how the affairs of government are conducted. The Restricted Data system established under the Atomic Energy Act and as operated by the Atomic Energy Commission was considered as a possible model for a new statutory system.

Executive Order 12065 (December 1978) - Seeking a Better Balance

The Carter Administration considered that Executive Order 11652 contained certain weaknesses and, as a result, an interagency review group was convened under the direction of Robert Gates, then a member of the NSC staff (later the Deputy to the National Security Adviser to the President, and now the Director of Central Intelligence). The interagency group produced Executive Order 12065 that was issued in June 1978 with an effective data of December 1978.

The major changes from the previous order were:

- A change to the definition of Confidential to require "identifiable damage" rather than merely "damage."

- A balancing test for classified information in order to determine whether the public interest in disclosure outweighs the damage to the national security.

- Established a policy that when reasonable doubt existed about which classification designation is appropriate, the less restrictive designation should be used.

- Identified seven areas with which information must be concerned in order for it to be classifiable.

- Established a six year maximum before automatic declassification, with provisions for exemptions.

- Abolished the Interagency Classification Review Committee and established the Information Security Oversight Office (ISOO) to monitor the classification activities of the Executive Branch. The NSC retained the overall policy direction for the order.

Executive Order 12356 (August 1982) - A More Conservative Approach

Because of some problems resulting from the implementation of E.O. 12065, an interagency group was convened under the direction of the Director of ISOO in 1980 during the Carter Administration to work on an amendment to the order. Certain provisions of the order such as the "identifiable damage" and the balancing test had proven to raise problems during litigation associated with Freedom of Information Act requests.

The interagency group continued their efforts after the Reagan Administration took over but their direction was changed from drafting a revision of E.O. 12065 to producing a new order, E.O. 12356, which was issued on April 6, 1982, with an effective date of August 1, 1982 (See Appendix E). The tone of E.O. 12356 was in the direction of a tighter classification regime than E.O. 12065, as indicated by the following examples:

E.O. 12065	E.O. 12356
• Reasonable doubt-use lower classification	• Reasonable doubt-use higher classification until reviewed
• Identifiable damage needed to classify information	• Reasonably expected to cause damage needed to classify information
• No provisions for reclassification of information	• Reclassification of information permitted under certain conditions

- Information may not be considered for classification unless it concerns specified categories
- Specifies need to balance the public's interest against national security

- Information shall be considered for classification if it concerns specified categories
- Implies a balancing of the public's interest and national security

E.O. 12356 is still in effect as originally issued in 1982. However an interagency group under the chairmanship of the Director of the Information Security Oversight Office is working on a new order.

Over the past 50 years that Executive Orders have been used to promulgate national security classification policy, a much more formal and organized system has evolved. While this system is subject to change by each new Presidential Administration, this has not always happened. Where a new order has been issued by a new administration, the changes have tended to be more a change in tone than in substance. However, the fact that a new Executive Order can be issued that changes classification policy for the government without congressional input, has caused some congressional support for a statutorily based classification system similar to that incorporated in the Atomic Energy Act for Restricted Data. Table B-1 (from "Security Classification of Information," Oak Ridge Gaseous Diffusion Plant, K/CG-1077/V1, Arvin S. Quist (September 1989)) gives a comparison of various features of the Executive Orders for classification of National Security Information. Differences between NSI and RD are summarized in Table B-2.

TABLE B-2

Differences Between RD and NSI

	RD	NSI
BASIS	Atomic Energy Act	Executive Order 12356
DEFINITION	"All data" in specified categories; includes both government and private information	Government data in specified categories identified by classification authorities
DECLASSIFICATION		
• Authority	Secretary of Energy, and his delegate. Coordinates with DOD on military utilization information and with CIA on foreign intelligence information	Original Classifier or the designated senior official
• Criterion	"may be published without undue risk to the common defense and security"	"disclosure [cannot] reasonably be expected to cause damage to the national security"
POLICY	DOE establishes basic policy consistent with the Atomic Energy Act	Each agency administers its own classification and declassification program consistent with E.O. 12356 and with oversight provided by the Information Security Oversight Office
PROCEDURES	DOE Office of Classification establishes centralized policy and procedures through program guides and orders	Each agency operates in a decentralized manner with classification guidance developed for each program

B.3 The DOE Classification System

Introduction

The DOE Classification System operates in accordance with the policies and procedures contained in the Atomic Energy Act (AEA) for RD and Executive Order 12356 for NSI. The system includes both government and contractor classification elements under the direction of the Secretary, the Under Secretary, and the Director of Office of Security Affairs, with day-to-day operational responsibility assigned to the Director of the Office of Classification (OC) as shown in Figure B-1.

The DOE Classification System is centralized with policy, procedures, orders, and guidance originating in the Office of Classification and disseminated to DOE Program Offices, Field Offices, and Contractor organizations. The classification program, although closely related to the DOE security program, is clearly separate and distinct. Classification identifies the information to be protected; security determines how to implement this protection. This distinction has existed from the earliest days of the Atomic Energy Commission because of a philosophy that classification and security should be separate so that the integrity of both programs is maintained.

Organization

The DOE responsibility for the classification of information under the authority of the Atomic Energy Act and Executive Order 12356 is carried out by the Office of Classification under the Office of Security Affairs. The Office of Classification carries out its functions and accomplishes its mission and goals through the work of the Director's Office supported by two divisions. The organizational structure of the Office of Security Affairs and the Office of Classification are shown in Figures B-2 and B-3.

Mission

The mission of the Office of Classification is to develop and implement policy for the classification and declassification of Restricted Data, Formerly Restricted Data, and National Security Information within DOE's jurisdiction in accordance with the requirements of the Atomic Energy Act of 1954, as amended, and applicable Executive Orders. The statute and Executive Order require continuous review of Restricted Data and other classified information to assure that information is properly classified and to determine what information may be declassified and disseminated in the interest of scientific and technical progress and the general public welfare without damage to the national security. In addition, the Office supports the nonproliferation objectives of the U.S. by shaping its classification policies to inhibit the spread of nuclear weapons, materials, and associated technologies through cooperative and coordinated classification policies with other nations.

CLASSIFICATION AUTHORITY FLOW

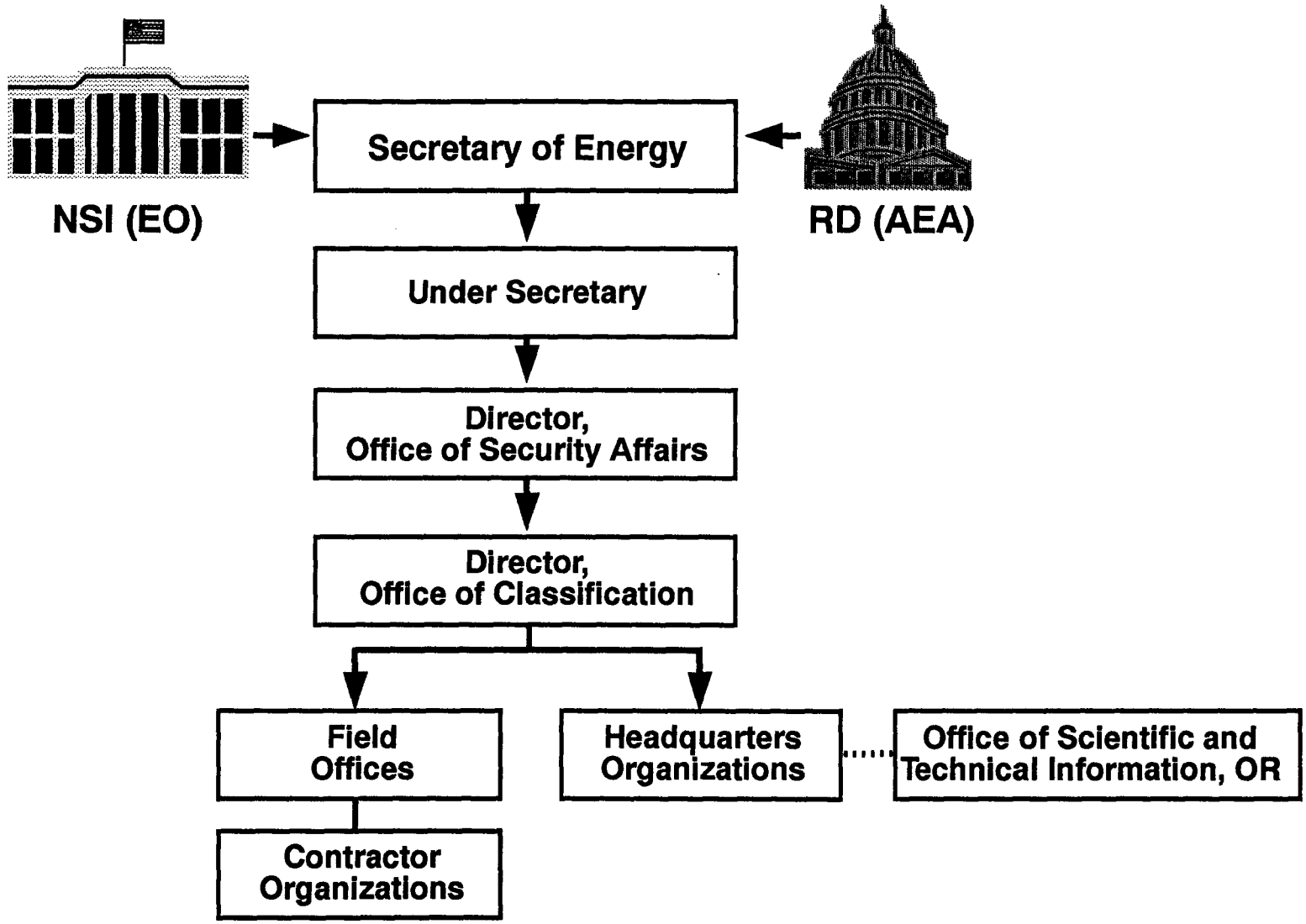


Figure B-1

ORGANIZATION OF THE OFFICE OF SECURITY AFFAIRS

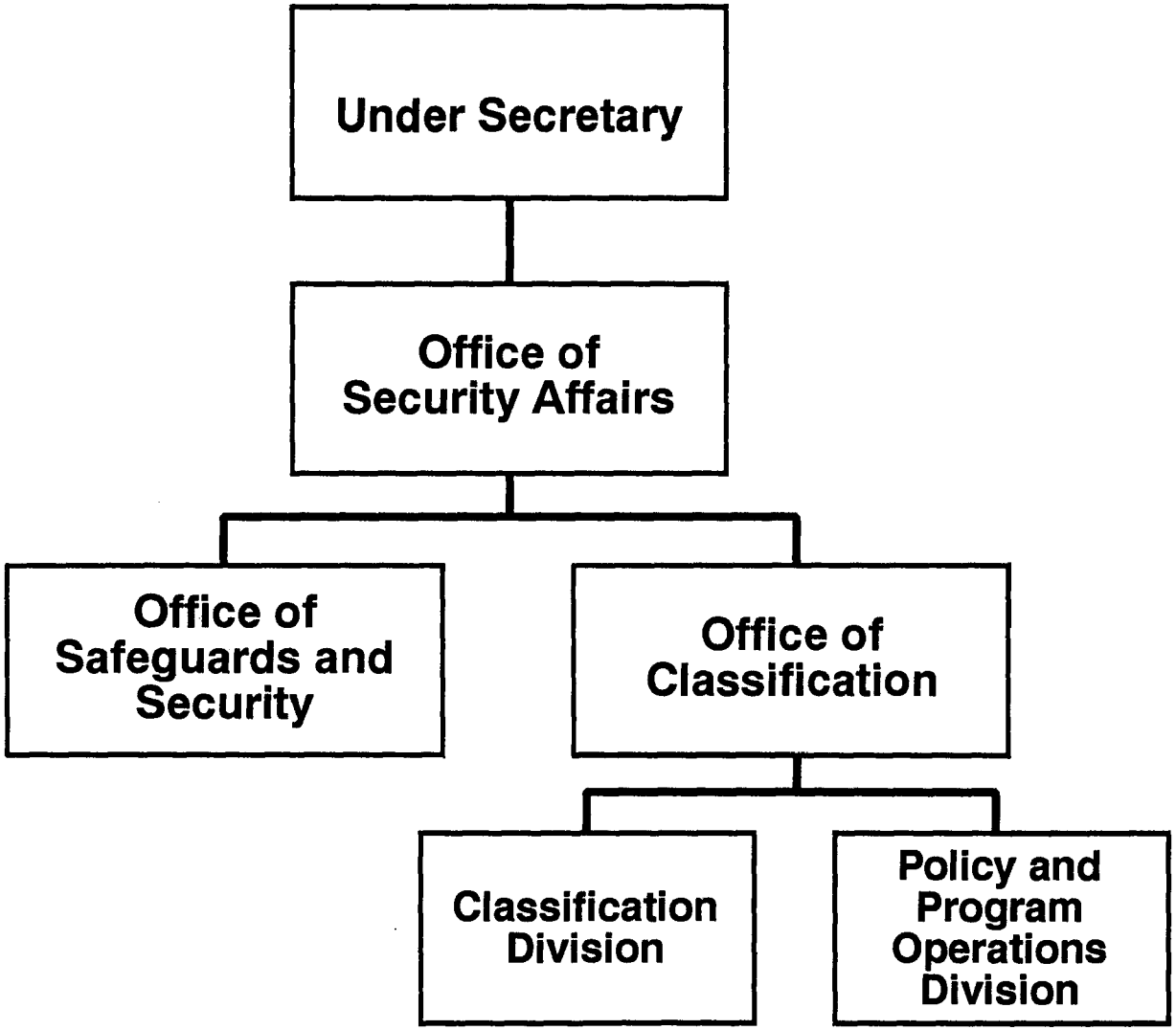


Figure B-2

ORGANIZATION OF THE OFFICE OF CLASSIFICATION

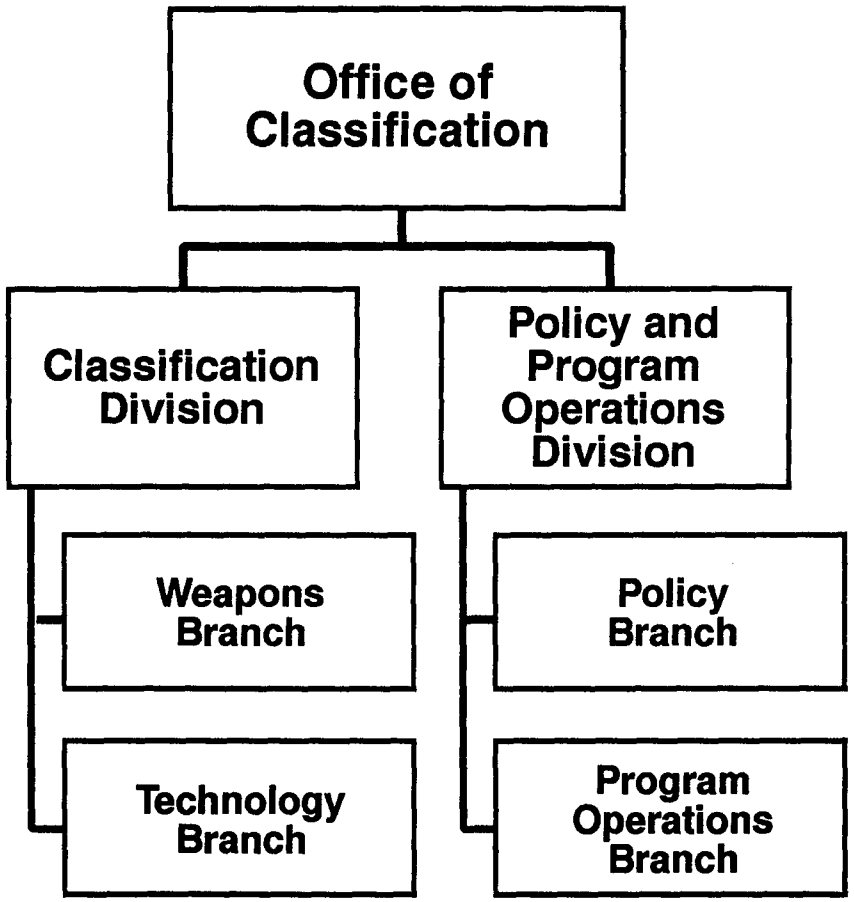


Figure B-3

Organizational Functions

The Office of Classification fulfills the above mission by carrying out the following functions:

- Develop, implement, and interpret DOE classification and declassification policy, guidance, rules, regulations, and procedures.
- Initiate and recommend to the Director of the Office of Security Affairs all actions for removing information from the RD and FRD (with DOD approval) categories.
- Perform interagency and international classification coordination and cooperation.
- Manage programs for classification and declassification review of documents and other materials.
- Develop classification and declassification education and training programs, and administer such programs for DOE headquarters personnel and, as required, for field element personnel.
- Appraise the effectiveness of the classification function of Departmental Elements and contractor organizations.
- Develop policies and procedures for the identification and control of Unclassified Controlled Nuclear Information (UCNI), as defined in sec. 148 of the AEA.

Program Activities

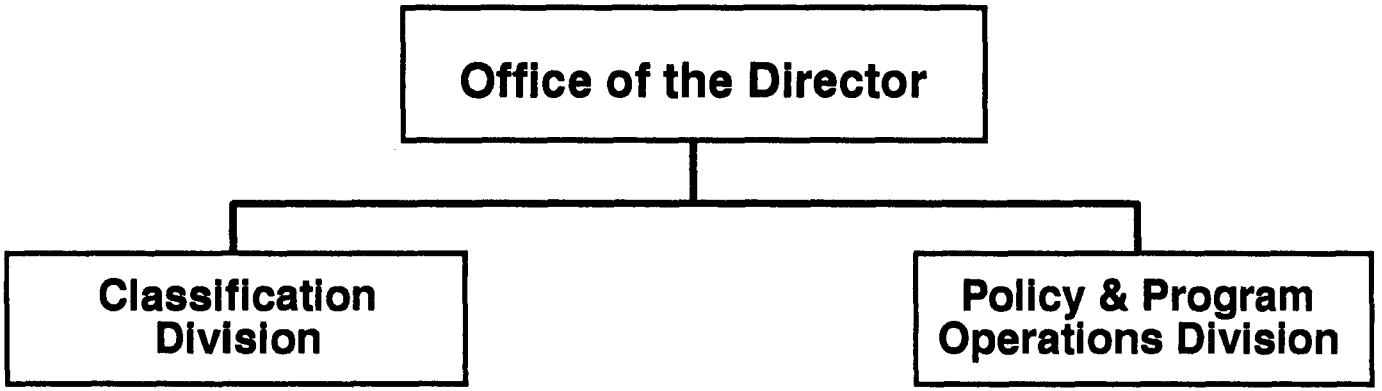
The Office of Classification carries out its functions and accomplishes its program goals through the work of the Director's office, supported by two divisions. The two divisions cover four major activities: (1) Classification Division (weapons activities and nuclear fuel cycle technology and safeguards activities); and (2) Policy and Program Operations Division (policy activities; and operational activities). See Figure B-4 for the responsibilities of the two divisions.

A. Classification Division Activities

Section 142 of the Atomic Energy Act requires that the DOE maintain a continuous review of Restricted Data and classification guides for atomic energy programs in order to determine which information may be declassified without undue risk to the common defense and security. Executive Order 12356 contains similar requirements regarding the issuance and periodic revision of classification guides for other programs.

The mission of the Classification Division is to meet this requirement by developing and implementing effective classification and declassification policies and guidance for specific DOE programs.

Office of Classification



- Nuclear Weapons
- Arms Control and Verification
- Intelligence
- Isotope Separation
- Production and Military Reactors
- Safeguards and Security
- Space Power
- Sensitive Non-Nuclear Technologies

- Basic Classification Policy
- Unclassified Controlled Information
- Regulations/Procedures
- Education/Training
- Appraisals
- Automation
- Document Reviews (FOIA)
- Program Planning/Budget

Figure B-4

To be effective, such policies and guidance must be scientifically credible, technically accurate, consistent with the statutory and Executive Order criteria, and practical from an operational viewpoint.

Program responsibility is divided between two branches: (1) The Weapons Branch, covering all nuclear weapon related program activities including nuclear directed energy weapons, nuclear emergencies, and ICF; and (2) The Technology Branch, covering all other DOE program activities requiring classification policy and guidance support, including both sensitive nuclear and non-nuclear technologies.

B. Policy and Program Operations and Support Division Program Activities

The mission of the Policy and Program Operations Division covers a broad spectrum of activities designed to (1) achieve consistent and effective basic overall classification policies and procedures; (2) ensure that information is properly classified and declassified in accordance with applicable statutes and Executive Orders; (3) provide timely and consistent document reviews; (4) develop and maintain the DOE education and training program; (5) develop and maintain management information systems including the computer-based Classification Guide System (CGS); (6) manage the Unclassified Controlled Nuclear Information (UCNI) program; (7) maintain quality assurance, program planning, budget, and contracting activities.

Program responsibility is divided between two branches: (1) the Policy Branch for basic overall classification policy and procedures and support activities; and (2) the Program Operations Branch for classification and declassification reviews and procedures. Additionally, the Policy and Program Operations Division is responsible for implementing the Classification Appraisal Program. The purpose of this program is to provide the management review and oversight necessary to ensure the effectiveness of the classification program.

Program Structure

A. Policy

DOE classification policy for RD and NSI is contained in the Atomic Energy Act, Executive Order 12356, DOE Order 5650.2B, Classification Guides, Classification Bulletins, and other policy documents.

1. General - The principle underlying classification and declassification policy for atomic energy information is to achieve a balance between two aims: (1) assuring the common defense and security by controlling the declassification of information concerning the military aspects of atomic energy; and (2) promoting the dissemination of scientific and technical information relating to the peaceful applications of atomic energy consistent with the common defense and security. However, the Atomic Energy Act states that the paramount objective of protecting the common defense and security must be observed. A determination on the declassification or downgrading of information can proceed only after a

careful balancing of the risk to the common defense and security against the benefit to a DOE program or the public welfare of the proposed action. In such a risk-benefit analysis, credibility of the DOE classification program is one of the factors considered. It is particularly important to avoid revealing information that may contribute to nuclear proliferation.

In accordance with E.O. 12356, it is DOE policy to classify information as NSI that concerns national defense and foreign relations which in the interest of the U.S. must be protected against unauthorized disclosure.

2. Classification Guides - DOE classification policy is implemented through a hierarchy of classification guides. In principle, the Policy Guide provides overall classification policy that serves as the basis for the Program Classification Guides that indicate the classification level of information within specific programs. Based on the Program Guides, Local Guides are developed by the DOE field offices and contractor organizations to provide detailed, site-specific classification guidance. There are over 800 classification guides of all types. The Policy Guide and Program Guides are issued by the Office of Classification while the Local Guides are issued by the DOE or contractor field elements. The local guides are approved by the Office of Classification except where that authority has been delegated to a Field Office. The DOE guide system helps to ensure consistent and accurate classification determinations.

3. Classification Bulletins - In general, the purpose of Classification Bulletins is the same as for Classification Guides, but with a more limited scope. Bulletins may express classification policy or clarify or expand guidance. Bulletins may also cover classification procedural matters.

4. UCNI Guidelines - The Office of Classification is also responsible for developing and issuing general and topical guidelines for the identification and control of UCNI. The guidelines cover DOE production and utilization facilities, safeguards and security information, and certain declassified nuclear weapons information.

B. Procedures

1. Classification and Declassification of RD and FRD - Since RD and FRD are classified by the Atomic Energy Act, there is no original classification determination required for this type of information. The authority to declassify RD and FRD has been delegated by the Secretary of Energy to the Director of the Office of Security Affairs. In the case of RD information relating to nuclear weapons, the DOE normally coordinates a declassification action with the DOD. FRD can only be declassified by the joint action of the DOE and the DOD. Once RD and FRD have been declassified they may not be reclassified as RD, FRD or NSI.

2. Criteria for Declassification - In formulating recommendations for declassification of RD and FRD, the following criteria are considered:

- The extent to which the information would assist potential adversaries in the development of an initial nuclear weapon capability or in improvements to existing nuclear weapons.
- The extent to which the information would assist others in countermeasures against U.S. nuclear weapons or in unauthorized use.
- The extent to which the information would assist in the production of special nuclear material (if applicable).
- The cost in terms of time and money of acquiring the information independently.
- The state of the art for the information in both the U.S. and in other countries.
- The benefit to be realized by the U.S. public welfare from the declassification, including improvements in environment, safety, and health and any significant technology commercialization potential.
- Any detrimental (or beneficial) effect that release of the information might have on U.S. foreign relations, arms control negotiations, or treaty obligations.
- Any impact on the credibility and effectiveness of the Department of Energy classification program caused by the continued classification of the information.
- Any penalties to U.S. programs due to the continued classification of the information.

3. NSI Classification and Declassification - In order for information to be classified as NSI it must concern at least one of the classifiable areas specified in E.O. 12356 (see Appendix E), and the unauthorized disclosure of the information must reasonably be expected to cause damage to the national security. In DOE, NSI may only be declassified by the original classifier of such information or by the Director of the Office of Classification.

4. Other Control Measures - Information determined to be unclassified according to topics in a classification guide is not automatically approved for release to the public. Unclassified information may be subject to a number of limitations on its distribution (e.g., proprietary information, patent review clearance, Naval Nuclear Propulsion Information (NNPI), Unclassified Controlled Nuclear Information (UCNI), and other exemptions under the Freedom of Information and the Privacy Acts). Review of all

applicable regulations and orders as required by the specifics of each case prior to the release of any unclassified information is the responsibility of the official authorizing the release.

5. Access to Classified Information - RD, FRD, and NSI may be transmitted only to persons having appropriate clearance and a valid need-to-know. RD or FRD may be transmitted to a foreign nation or a regional defense organization only if there is a formal Agreement for Cooperation between the receiving party and the U.S., entered into in accordance with the provisions of section 123 of the Atomic Energy Act of 1954, as amended, and implementing statutory determinations under sections 91 c., 144 b., and 144 c., as appropriate.

Critical Nuclear Weapon Design Information (CNWDI) is an access limiter used primarily within the DOD to control need-to-know access for nuclear weapon design information (See Appendix F). DOE uses a Sigma numbering system to identify Nuclear Weapon Data (see Table B-3) that is classified RD or FRD. For example, the Sigma 1 category covers information concerning the theory of operation or complete design of thermonuclear weapons or their unique components. Information in a Sigma category may be made available only to individuals approved to receive that category of information.

C. DOE Classification Community

The Office of Classification (OC) provides oversight and guidance to the DOE classification community consisting of Classification Officers at the DOE Field Offices and major classified contractors. There are Classification Officer meetings sponsored by OC that are held three times a year to discuss classification issues of mutual interest. These are especially useful in keeping OC and the field organizations aware of each other's concerns and problems related to classification. These meetings are supplemented by periodic visits by OC management to field organizations in order to improve communications between OC and the field and to increase field office and contractor management awareness of the classification program.

D. Interagency Activity (See Figure B-5)

The OC maintains a working relationship with other government departments and agencies on classification matters. The most extensive coordination is carried out between DOE and DOD because of the joint responsibility for FRD contained in the Atomic Energy Act and because of nuclear weapons-related classification guidance and other related matters.

TABLE B-3

SIGMA CATEGORIES
(Weapons Data Access Designators)

SIGMA CATEGORIES. Restricted Data and/or Formerly Restricted Data in the following categories which concern the design, manufacture, or utilization of atomic weapons or nuclear explosive devices:

Sigma 1. Theory of operation (hydrodynamic and nuclear) or complete design of thermonuclear weapons or their unique components.

Sigma 2. Theory of operation or complete design of fission weapons or their unique components. This includes the high explosive system, and nuclear initiation system as they pertain to weapon design and theory.

Sigma 3. Manufacturing and utilization information not comprehensively revealing the theory of operation or design of the physics package. Complete design and operation of nonnuclear components but only information as prescribed below for nuclear components. Utilization information necessary to support the stockpile to target sequence. Information includes:

(a) general external weapon configuration, including size, weight, and shape.

(b) environmental behavior, fuzing ballistics, yields, and effects.

(c) nuclear components or subassemblies which do not reveal theory of operation or significant design features.

(d) Production and manufacturing techniques relating to nuclear parts or subassemblies.

(e) anticipated and actual strike operations.

Sigma 4. Information inherent in preshot and post-shot activities necessary in the testing of atomic weapons or devices. Specifically excluded are the theory of operation and the design of such items. Information includes:

(a) logistics, administration, other agency participation.

(b) special construction and equipment.

(c) effects, safety.

(d) purpose of tests, general nature of nuclear explosive tested including expected or actual yields and conclusions derived from tests not to include design features.

Sigma 5. Production rate and/or stockpile quantities of nuclear weapons and their components.

Sigma 9. General studies not directly related to the design or performance of specific weapons or weapon systems, e.g., reliability studies, fuzing studies, damage studies, aerodynamic studies, etc.

Sigma 10. Chemistry, metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices.

Sigma 11. Information concerning inertial confinement fusion which reveals or is indicative of weapon data.

Sigma 12. Complete theory of operation, complete design, or partial design information revealing either sensitive design features or how the energy conversion takes place for the nuclear energy converter, energy director or other nuclear directed energy weapon systems or components outside the envelope of the nuclear source but within the envelope of the nuclear directed energy weapon.

Sigma 13. Manufacturing and utilization information and output characteristics for nuclear energy converters, directors and other nuclear directed energy weapon systems or components outside the envelope of the nuclear source, not comprehensively revealing the theory of operation, sensitive design features of the nuclear directed energy weapon or how the energy conversion takes place. Information includes:

(a) General external weapon configuration and weapon environmental behavior characteristics, yields, and effects.

(b) Component or subassembly design that does not reveal theory of operation or sensitive design features of nuclear directed energy weapons categorized as Sigmas 1, 2, or 12.

(c) Production and manufacturing techniques for components or sub-assemblies of nuclear directed energy weapons that do not reveal information categorized as Sigmas 1, 2, or 12.

OC RELATIONSHIPS WITH OTHER AGENCIES

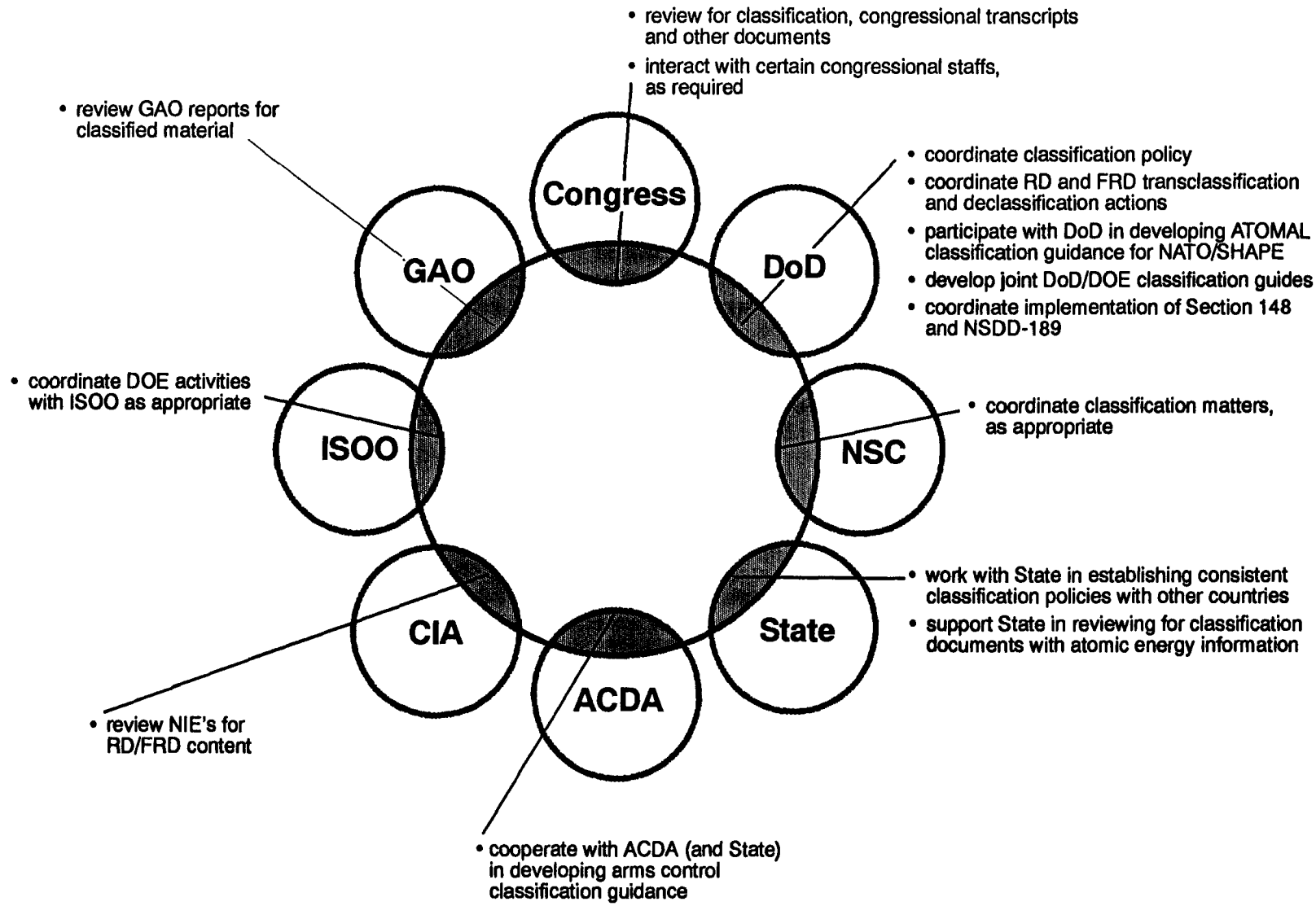


Figure B-5

E. International Activities (See Figure B-6)

Coordination is maintained between OC and those responsible for classification in the UK, France, and Canada. The Policy Guide is coordinated with the UK and Canada, and the US and UK coordinate on and issue a joint weapons classification guide.

OC has also maintained coordination with the UK, FRG, and the Netherlands on the classification of gas centrifuge enrichment technology. This relationship results in similar classification policies among the four governments for centrifuge technology.

General classification policies are also coordinated among the U.S., UK, and France for ICF information.

F. Technical Evaluation Panel

The Technical Evaluation Panel consists of a group of senior classification advisors to the Director of the Office of Security Affairs. It succeeded the "Committee of Senior Reviewers" in 1978. Each of the three weapon laboratories (LANL, LLNL, and SNL) is represented by a member of the panel, and a retired senior military officer with relevant experience serves as a consultant.

OC RELATIONSHIPS WITH FOREIGN ENTITIES

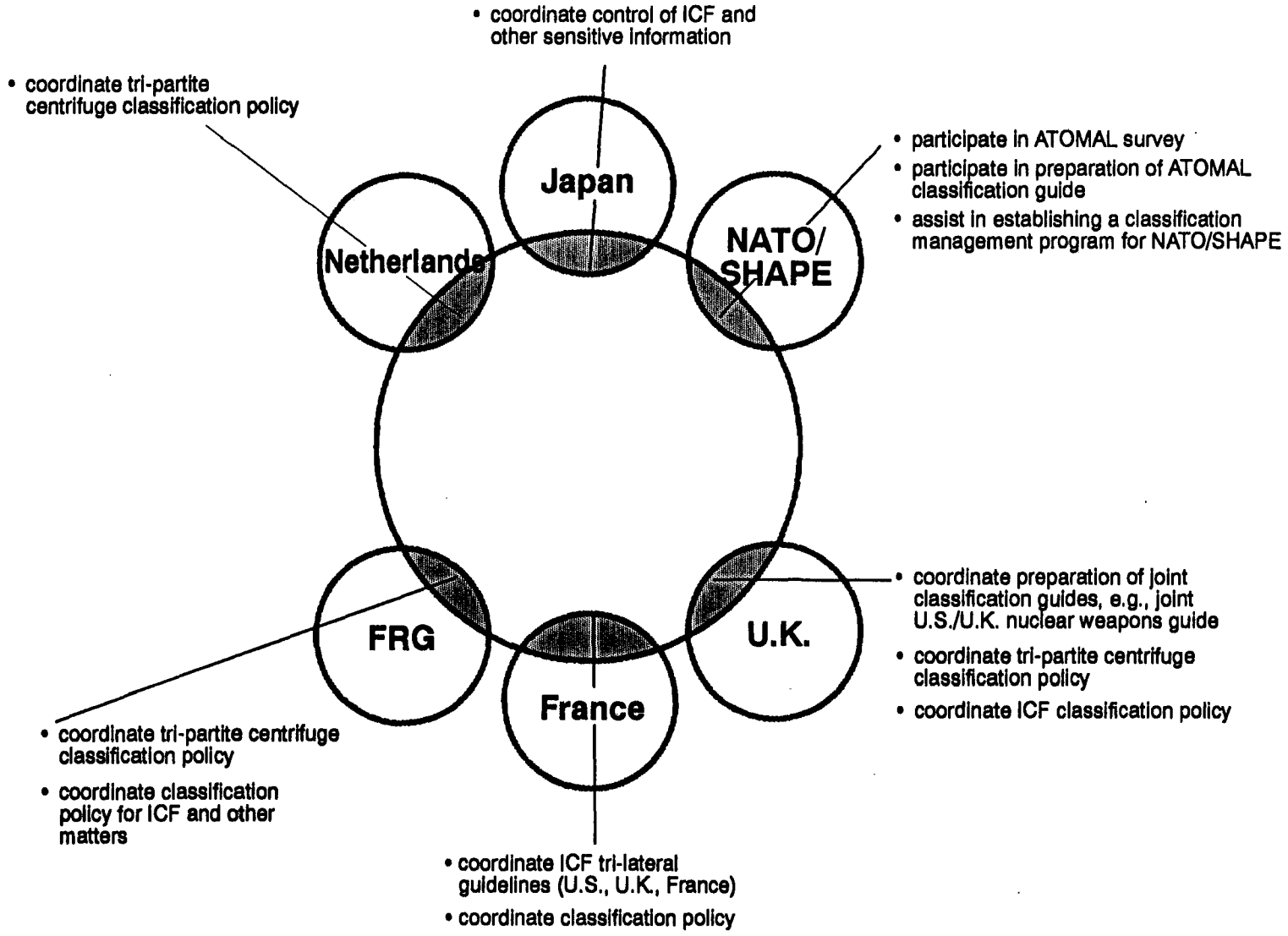


Figure B-6

APPENDIX C

Principal Contacts for Classification Policy Study*

1. DOE

Headquarters

AD - Administration and Human Resource Management
  - Office of Scientific and Technical Information
  - History Division
AN - Arms Control and Nonproliferation
DP - Defense Programs: Military Applications
  - Development, Testing, and Acquisition
  - Transportation Safeguards and Emergency Management
  - Research and Advanced Technology
EH - Environment, Safety, and Health
EM - Environmental Restoration and Waste Management
ER - Energy Research
GC - General Counsel
NE - Nuclear Energy
  - Uranium Enrichment
SA - Security Affairs
  - Safeguards and Security
  - Classification

Field Offices

Albuquerque (AL)
Chicago (CH)
Idaho (ID)
Nevada (NV)
Oak Ridge (OR)
Rocky Flats (RF)
Richland (RL)
San Francisco (SAN)
Savannah River (SR)

*Listed by institutional affiliation. In many cases several people were interviewed, including managers and staff of technical programs and classification offices. Both group and individual interviews were used.

Laboratories

Argonne National Laboratory (ANL)
Brookhaven National Laboratory (BNL)
Los Alamos National Laboratory (LANL)
Lawrence Livermore National Laboratory (LLNL)
Oak Ridge National Laboratory (ORNL)
Pacific Northwest Laboratory (PNL)
Sandia National Laboratories; Albuquerque and Livermore (SNLA, SNLL)
Idaho National Engineering Laboratory (INEL)

Other Major DOE Contractors

Pinellas - General Electric Nuclear Devices (GEND)
Kansas City - Allied-Signal Aerospace Co., Kansas City Division (KCD)
Nevada Test Site (NTS) - Reynolds Electrical and Engineering Co. (REECO), EG&G, Holmes and Narver
Rocky Flats (RF) - EG&G
Y-12 - Martin Marietta Energy Systems (MMES)
Savannah River - Westinghouse, Wackenhut
PANTEX - Mason Hanger - Silas Mason
MOUND - EG&G
Idaho - EG&G, Westinghouse Idaho Nuclear Co. (WINCO), Rockwell
Richland - Battelle, Westinghouse, Rockwell, Kaiser
K-25 - Martin Marietta Energy Systems (MMES)
Paducah-MMES
Portsmouth-MMES

2. OTHER EXECUTIVE AGENCIES

Arms Control and Disarmament Agency (ACDA)
Central Intelligence Agency (CIA)
Department of Defense (DOD)
Department of Justice (DOJ)
Department of State (DOS)
Institute for Defense Analysis (IDA)
Information Security Oversight Office (ISOO)
National Science Foundation (NSF)
Nuclear Regulatory Commission (NRC)
Office of Management and Budget (OMB)

3. CONGRESS

House
- Armed Services (HASC)
- Energy and Commerce (HE&C)

Senate
- Governmental Affairs (SGA)
- Armed Services (SASC)

4. Interest Groups

- American Civil Liberties Union (ACLU)
- Carnegie Institution
- Federation of American Scientists (FAS)
- Nuclear Control Institute (NCI)
- Natural Resources Defense Council (NRDC)
- Union of Concerned Scientists (UCS)

5. Professional Societies

- American Association for the Advancement of Science (AAAS)
- American Chemical Society (ACS)
- American Institute of Aeronautics and Astronautics (AIAA)
- American Nuclear Society (ANS)
- American Physical Society (APS)
- American Society of Mechanical Engineers (ASME)
- Institute of Electrical and Electronic Engineers (IEEE)
- National Academy of Engineering (NAE)
- National Academy of Science (NAS)
- Optical Society of America (OSA)
- Society of Manufacturing Engineers (SME)

6. Trade and Other Associations

ADAPSO, The Computer Software and Services Industry Association
Adhesive and Sealant Council
Aerospace Industries Association
Alliance of Metal Working Industries
American Association of Ceramic Industries
American Council of Independent Laboratories
American Electronics Association
American Iron & Steel Institute
Association of American Universities (AAU)
Association of Industrial Metalizers, Coaters, and Laminators
Association of Small Research, Engineering, and Technical Services
Center for Innovative Technology
Chemical Manufacturers Association
Computer and Communications Industry Association
Council on Competitiveness
Council on Research and Technology
Electronic Industries Association
Electric Power Research Institute
Federal Laboratory Consortium
Industrial Research Institute
Los Alamos Economic Development Corporation
NMBTA -- Association for Manufacturing Technology
National Association of Manufacturers
National Electrical Manufacturers Association
National Machine Tool Builders Association
Oak Ridge Associated Universities

Trade and Other Associations (Cont'd)

Precision Metalforming Association
Resources for the Future
Specialty Metals Processing Consortium
Technical Ceramics Manufacturing Association
Technology Transfer Society
U.S. Advanced Ceramics Association
U.S. Council for Energy Awareness

7. Advisory Committees

- Advisory Committee on Nuclear Facility Safety (ACNFS)
- Defense Nuclear Facilities Safety Board (DNFSB)

8. Former Government Officials

- AEC/ERDA/DOE
  - LANL
  - LLNL
- ACDA
- DOS
- DOD

APPENDIX F

Glossary

ACRONYMS

AEA - The Atomic Energy Act of 1954, as amended.

ACDA - The Arms Control and Disarmament Agency.

AEC - The Atomic Energy Commission.

ASDP - The Assistant Secretary of Energy for Defense Programs (also "DP-1").

CNWDI - Critical Nuclear Weapon Design Information.

DP-1 - The Assistant Secretary of Energy for Defense Programs (also "ASDP").

EO - Executive Order.

FOIA - Freedom of Information Act of 1967, as amended.

FOUO - For Official Use Only, a category of unclassified but sensitive information used by the Department of Defense.

FRD - Formerly Restricted Data.

GAO - General Accounting Office.

ICF - Inertial Confinement Fusion.

ISOO - Information Security Oversight Office.

LOU - Limited Official Use, a category of unclassified but sensitive information in the Department of State.

NDP - National Disclosure Policy.

NDPC - National Disclosure Policy Committee.

NIE - National Intelligence Estimate.

NISP - National Industrial Security Program.

NNPA - Nuclear Non-Proliferation Act of 1978.

NNPI - Naval Nuclear Propulsion Information.

NPT - Non-Proliferation Treaty: "Treaty on the Non-Proliferation of Nuclear Weapons" (1970).

ACRONYMS (Cont'd)

NSC - National Security Council.

NSI - National Security Information.

OC - Office of Classification, Security Affairs, DOE (formerly Office of Classification and Technology Policy (OCTP)).

OCTP - Former Office of Classification and Technology Policy in Defense Programs, DOE (now Office of Classification (OC)).

OSA - Office of Security Affairs, DOE.

OSS - Office of Safeguards and Security, DOE.

OUO - Official Use Only.

RD - Restricted Data.

S-1 - The Secretary of Energy.

S-2 - The Deputy Secretary of Energy.

S-3 - The Under Secretary of Energy.

SA-1 - The Director of the Office of Security Affairs.

SA-20 - The Director of the Office of Classification.

SCI - Sensitive Compartmented Information.

SUCI - Sensitive Use Control Information.

TEP - Technical Evaluation Panel.

TS - Top Secret.

UCNI - Unclassified Controlled Nuclear Information.

WD - Weapon Data.

DEFINITIONS

A

Agreement for Cooperation - Any agreement with another nation or regional defense organization authorized under sec. 123 of the AEA.

Atomal - The term NATO uses for classified military nuclear information that corresponds to U.S. RD/FRD.

Atomic Energy Act (AEA) - The Atomic Energy Act of 1954, as amended.

Atomic Energy Commission (AEC) - A five-member commission and supporting organization established by the AEA of 1946 to manage the U.S. civil and military nuclear energy programs. Succeeded by the Energy Research and Development Agency (ERDA) in 1974 and then by the current Department of Energy (DOE) in 1977.

B

"Born Classified" - The term used to describe the fact that Restricted Data information is classified by the AEA from its origin. No affirmative act of classification is necessary with RD, as it is with NSI.

C

Classification - The determination by an authorized official that information requires protection under the provisions of an Executive Order (NSI) or that a document or material contains NSI or contains Restricted Data (RD) or Formerly Restricted Data (FRD), as defined in the Atomic Energy Act.

Classification Category - One of the three kinds of classified information (i.e., RD, FRD, or NSI).

Classification Guide - A document containing explicit classification guidance.

Classification Level - One of the three terms which indicate the degree of sensitivity of classified information, i.e., Top Secret, Secret, or Confidential.

Classification Officer - Official who administers classification programs of a Field Element or contractor and oversees or monitors classification programs of contractors under their jurisdiction.

Clearance - See "Security Clearance".

Commission - The former Atomic Energy Commission. As used in the AEA, now generally the Secretary of Energy.

Confidential (C) - The lowest classification level, applied to information whose unauthorized disclosure could reasonably be expected to cause damage to national security.

Critical Nuclear Weapon Design Information (CNWDI) - A Department of Defense (DOD) category of weapon data designating Top Secret/Restricted Data or Secret/Restricted Data revealing the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded from designation as CNWDI is information concerning:

(1) Arming, fuzing, and firing systems.
(2) Limited life components.
(3) Total contained quantities of fissionable, fusionable, and high explosive materials by type.
(4) Components which military personnel set, maintain, operate, test, or replace.

D

Declassification - A determination by appropriate authority in accordance with approved classification policy that information is no longer classified, or that a document or other material no longer contains classified information.

Derivative Classification - A determination in accordance with approved classification guidance or source documents that a document or material is classified (NSI, RD, or FRD).

Document - Any record of information regardless of physical form.

Downgrading - A determination by appropriate authority that the level or category of classified information, documents, or material may be lowered to reflect reduced expectations of damage from unauthorized disclosure, e.g., reducing the level from Top Secret to Secret, or from Secret to Confidential.

E

Executive Order (EO) - Formal Presidential order mandating activities of the Executive Branch. As used here, Executive Orders concern the identification and protection of classified national security information, such as the current Executive Order 12356.

F

Field Element - A departmental element located outside the Metropolitan Washington area.

Foreign Government Information - Information provided to the U.S. in confidence by foreign governments or developed by the U.S. under arrangements with foreign governments requiring confidentiality.

Formerly Restricted Data - Classified information jointly determined by DOE and DOD to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category pursuant to section 142 d. of the Atomic Energy Act. FRD is protected as NSI except for the purpose of foreign dissemination where it is treated as RD.

G

Guide - See "Classification Guide".

I

Information Security Oversight Office (ISOO) - An organization within the General Services Administration responsible for implementing and monitoring the information security program prescribed in E.O. 12356. The National Security Council provides overall policy direction for this program.

International Arrangement - Any international agreement approved by the Congress or any treaty. Agreements for Cooperation are not included.

L

L-Clearance - DOE or NRC clearance for access to CRD, SFRD, SNSI. Not used for DOE employees.

Local Classification Guide - A classification guide prepared and issued by DOE or by a DOE contractor organization and approved by DOE for a specific facility or activity. It is based on one or more Program Classification Guides and provides detailed classification guidance.

M

Mandatory Review - A declassification review that can be initiated or requested by a member of the public, a Government employee, or another Government agency pursuant to E.O. 12356.

N

National Disclosure Policy (NDP) - Presidentially approved policy concerning communication of classified military information to foreign governments.

National Disclosure Policy Committee (NDPC) - Interagency committee established to apply the National Disclosure Policy.

National Industrial Security Program (NISP) - A major Executive Branch program to establish government-wide standards and procedures for industrial security for government contracts.

National Security - The national defense and foreign relations of the United States.

National Security Information (NSI) - Information that has been determined pursuant to Executive Order 12356 or any predecessor order to require protection against unauthorized disclosure and that is so designated. Note that only DOE uses "NSI" markings on documents.

Naval Nuclear Propulsion Information (NNPI) - Information, classified or unclassified, concerning the Naval Nuclear Propulsion Program.

Need-To-Know - A determination by a person having responsibility for classified information or material that a proposed recipient's access to such classified information or matter is necessary in the performance of official or contractual duties of employment.

Nuclear Non-Proliferation Act of 1978 (NNPA) - Public Law 95-242 (March 10, 1978) provides for additional controls over sensitive nuclear weapons-related technology.

O

Official Use Only (OUO) - A designation identifying certain unclassified DOE information that may be exempt from public release under the FOIA.

Original Classification - The initial determination that information requires protection as NSI under the provisions of Executive Order 12356. Includes the specification of a classification level and the classification duration.

P

Policy Guide - A guide by which the Director of the Office of Security Affairs approves basic DOE policy statements on the classification and declassification of all DOE nuclear-related information.

Private Restricted Data - Information meeting the AEA definition of Restricted Data but generated outside government control.

Program Classification Guide - A guide that states specific classification policy for a particular DOE program and provides the basis for the development of local guides.

Proliferation - Used here to describe both first acquisition and subsequent developments of nuclear explosives by other countries.

Q

Q-Clearance - DOE or NRC clearance for SRD, TSFRD, TSNSI. A "Q-sensitive" clearance and written authorization by designated senior officials are required for TSRD.

R

Restricted Data (RD) - A category of classified information defined by the AEA, Sec 11.y.: "The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142."

Responsible Reviewers - Reviewers appointed to advise Field Element and contractor Classification Officers and SA-20 on matters in their field of professional expertise.

S

Secret (S) - The classification level between Confidential and Top Secret, applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Security - The protection of valuable matter, including classified material and information.

Security Clearance - Official determination that access by an individual to classified information will not be inimical to national security, e.g., in DOE (and NRC) "L-" and "Q"-clearances for RD, FRD and NSI, and "S" and "TS" clearances for NSI only. "C", "S", and "TS" clearances are used in other agencies for NSI.

Sensitive Compartmented Information (SCI) - Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Use Control Information (SUCI) - Particularly sensitive information concerning possible circumvention of nuclear weapon use control features.

Sensitive Nuclear Technology (SNT) - Information on uranium enrichment, nuclear fuel reprocessing, and heavy water production whose export is controlled under the NNPA, i.e., such information that is not RD, not publicly available, and important to design, construction, operation, or maintenance of related facilities.

Sigma Categories - Designations used for access control, or need-to-know, for Restricted Data and/or Formerly Restricted Data in various categories which concern the design, manufacture, or utilization of atomic weapons, or utilization of atomic weapons or nuclear explosive devices. (See Table B-3 of Appendix B.2.)

Special Nuclear Material (SNM) - Plutonium, uranium enriched in the isotopes 233 or 235, or any material enriched in the foregoing.

T

Technical Evaluation Panel (TEP) - A panel of senior technical experts appointed to advise SA-1 on the technical aspects of information under the cognizance of the Office of Classification.

Top Secret (TS) - The highest classification level, applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.

Transclassification - The removal of information from the RD category to (1) the FRD category (military utilization information, section 142 d. of the AEA) or (2) the NSI category (foreign intelligence information, section 142 e. of the AEA.

U

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

Unclassified Controlled Nuclear Information (UCNI) - Certain unclassified Government information prohibited from unauthorized dissemination under sec. 148 of the AEA.

Upgrading - Raising the classification level and/or category of (1) information or (2) documents or material, including correction of classification of such items erroneously issued as unclassified or at too low a classification level or category.

W

Weapons Data (WD) - Restricted Data/Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or atomic weapon components. This includes information incorporated in or relating to nuclear explosive devices.

APPENDIX G

Bibliography

7.1 PUBLIC LAWS

- Public Law 82-593, "The Patent Secrecy Act of 1952" [established authority for imposing secrecy on patents of importance to the national security]

- Public Law 83-703, "The Atomic Energy Act of 1954, as amended," 42 U.S.C. 201, (August 30, 1954)[established requirements for availability and dissemination of information generated by or for DOE]

- Title 5 U.S.C. 552, "The Freedom of Information Act" (1966)

- Public Law 93-438 "The Energy Reorganization Act of 1974, as amended" (October 11, 1974) [created the Energy Research and Development Administration (ERDA) and the Nuclear Regulatory Commission (NRC)]

- Public Law 95-91, "The Department of Energy Organization Act of 1977," 42 U.S.C. 7112(5)(d) (August 4, 1977) [created the Department of Energy and established requirements for dissemination of information generated by or for DOE.]

- Public Law 95-242, "The Nuclear Non-Proliferation Act of 1978" (March 10, 1978) [provided for more efficient and effective control over the proliferation of nuclear explosive capability.]

- Public Law 96-480, the Stevenson-Wydler Technology Innovation Act of 1980 (October 21, 1980), [requires technology transfer by federally funded R&D laboratories to state and local governments and to the private sector]

- "Defense Technical Data Act", A section of the Department of Defense Authorization Act of 1984

- Public Law 102-228, "The Soviet Nuclear Threat Reduction Act of 1991" (SNTRA) (November 1991)

7.2 EXECUTIVE ORDERS

- Executive Order 12356, "National Security Information" (April 6, 1982)

- NSDD 189, "National Policy on the Transfer of Scientific Technical, and Engineering Information" (September 21, 1985) [provided national policy on the transfer of scientific, technical, and engineering information]

7.3 DEPARTMENTAL ORDERS

- DOE Order 1430.1A, "Managing Scientific and Technical Information" (September 10, 1986)
- DOE Order 1430.2, "Implementation of the Scientific and Technical Information Management Program" (December 13, 1983)
- DOE Order 1430.3, "Policy for the Dissemination of and Access to Departmental Unclassified Scientific and Technical Information" (December 24, 1986)
- DOE Order 1700.1, "Freedom of Information Program" (November 19, 1979)
- DOE Order 5610.2, "Control of Weapon Data" (August 1, 1980)
- DOE Order 5630.8A "Safeguarding of Naval Nuclear Propulsion Information" (July 31, 1990)
- DOE Order 5631.2B, "Personnel Security Program" (May 18, 1988)
- DOE Order 5631.4 "Control of Classified Visits" (May 25, 1984)
- DOE Order 5631.5, "Violation of Laws, Losses, and Incidents of Security Concern" (February 12, 1988)
- DOE Order 5632.5, "Physical Protection of Classified Matter" (February 3, 1988)
- DOE Order 5635.1A, "Control of Classified Documents and Information" (February 12, 1988)
- DOE Order 5635.4, "Protection of Unclassified Controlled Nuclear Information" (February 1988)
- DOE Order DP 5650.1, "Identification of Defense Programs Official Use Only Information" (September 12, 1990)
- DOE Order SA 5650.1, "Identification of Security Affairs Official Use Only Information (September 12, 1991)
- DOE Order 5650.2B, Identification of Classified Information (December 31, 1991) [Basic Directive for DOE Classification System]
- DOE Order 5650.3, "Identification of Unclassified Controlled Nuclear Information", (February 29, 1988)
- DOD Directive 5210.2 Rev., "Access to and Dissemination of Restricted Data", (January 12, 1978)

- Information Security Oversight Office Directive No. 1, "National Security Information" (June 23, 1982) [Supplement to E.O. 12356]

7.4 REGULATIONS

- Title 10 CFR 810, "Unclassified Activities in Foreign Atomic Energy Programs" (December 10, 1986) [Establishes control regulations for the Nuclear Non-Proliferation Act of 1978]

- Title 10 CFR 1017, "Identification and Protection of Unclassified Controlled Nuclear Information" (April 22, 1985) [Establishes overall policies and procedures for the identification and protection of Unclassified Controlled Nuclear Information (UNCI)]

- Title 15 CFR 368.1-399.2, "U.S. Export Administration Regulations" (including EAR 378.3, "Nuclear Technical Data" and EAR 379.4, "Technical Data") (April 25, 1980) [implements the Export Administration Act (50 U.S.C. App. Section 2401, et seq.), provides for development by DOD of a "Militarily Critical Technologies List" (MCTL)]

- Title 22 CFR 121-130, "Revision of the International Traffic in Arms Regulations" (ITAR) (April 1, 1985) [implements the Arms Control Export Act of 1976, as amended (22 U.S.C. 2728).]

7.5 REPORTS

- "A General Account of the Development of Methods of Using Atomic Energy for Military Purposes under the Auspices of the United States Government, 1940-45," H.D. Smyth, USGPO, Washington, (August 1945)

- "Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices" (November 1985)

- "The National Industrial Security Program: A Report to the President by the Secretary of Defense" (October 1990)

- "Nuclear Weapons Complex Reconfiguration Study" DOE/DP-0083 (January 1991)

- "Report of the Secretary's Safeguards and Security Task Force," Major General James E. Freeze, USA (Ret), et al. (December 1990)

- "National Energy Strategy," First Edition 1991/1992 DOE, (February 1991)

- "Security Classification of Information, Volume 1. Introduction, History, and Adverse Impacts," Oak Ridge Gaseous Diffusion Plant, K/CG-1077 V1, Arvin S. Quist (September 1989)

- "Scientific Communication and National Security" National Academy Press (September 1982)
- "Striking a Balance: National Security and Scientific Freedom," Harold C. Relyea (ed.), American Association for the Advancement of Science (May 1985)
- "Nuclear Weapons Information Study," Richard N. Cody, et al. (July 30, 1988)
- "National Security Controls and University Research: Selected Readings," Association of American Universities (June 1987)
- "Communicating Technical Information," American Institute of Aeronautics and Astronautics (January 1984)
- "The First Amendment and the Export Laws: Free Speech on Scientific and Technical Matters," Allen M. Shinn, Jr., George Washington Law Review 368 (1990)
- "Born Classified in the AEC: A Historian's View," Richard G. Hewlett, Bulletin of the Atomic Scientists (December 1981)
- "Born Classified in the AEC: A Legal Perspective," Harold P. Green, Bulletin of the Atomic Scientists (December 1981)