93-F-1443

DEPARTMENT OF DEFENSE
WASHINGTON, THE DISTRICT OF COLUMBIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY COUNTERMEASURES STRATEGIC PLAN (CI&SCM Strategic Plan)

Implementation Objective No. 1

A Report to the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

prepared by the

Directorate of Information Systems Security

Office of the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures)

April 1993

#496

CONTENTS

- Executive Summary 2
- Implementation Objective No. 1 4
- Action Plan 5
- Review and analysis of statutory information protection systems
  - Histories and analysis 7
    - Freedom of Information Act 7
    - DoD Authorization Act of 1984 10
    - Computer Security Act of 1987 11
    - Section 128 of title 10, United States Code 12
    - National Security Agency Act of 1959 12
    - Central Intelligence Agency Act of 1949 13
    - Atomic Energy Act of 1954 13
    - Other laws 13
  - Comparison of Statutes 13
  - Identification Processes 14
- Review and analysis of security classification system
  - History 16
  - Comparison of contemporary Executive orders 21
  - Identification Processes 26
    - Original Classification Policy 26
    - Original Classification Practice 30
    - Derivative Classification Policy 32
    - Derivative Classification Practice 33
- Definition of approach to be used in identifying and prioritizing categories of information needing protection 35
- Acting ASD(C3I) approval 37
- Appendices
  - ASD(C3I) Memorandum of June 4, 1992 A
  - Selected Statutes B
  - Executive Order 12356 C
  - Selected DoD Issuances D

EXECUTIVE SUMMARY

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) in the "Defense Counterintelligence and Security Countermeasures Plan"[1] calls for a new look at confidentiality of DoD information -- what information needs to be protected, how much protection is needed, and the duration of that protection. The ASD(C3I) mandates a review of the processes used for classification of information and designation of sensitive information, and development of an integrated approach -- to include establishing a senior review panel to provide cohesive and overall policy guidance -- that identifies, defines, and prioritizes the categories of information that require protection. Accomplishment of these objectives will enable DoD organizations to allocate their shrinking security resources to the most critical areas, thereby improving the overall protection of sensitive DoD information resources.

This report deals with two actions derived from the foregoing requirements (which are referred to collectively as Implementation Objective No. 1). They are:

- Review the processes for determining classification of information and designation of sensitive information; and

- Define the approach to be used in identifying/defining categories that need protection and prioritize the categories.

Other actions required to satisfy Implementation Objective No. 1 are set forth in the action plan that is a part of this report.

Information in the possession of the Department of Defense or its Components is held in trust for, or on behalf of, the citizens of the United States, and will be made available on request in accordance with the Freedom of Information Act (FOIA) except when laws or implementing regulations specifically require that its dissemination be limited. Information is a strategic asset vital to the performance of the missions of the Department of Defense. As a strategic asset, information must be protected to an extent and for a period commensurate with its value and the degree of danger posed by its unauthorized disclosure, misuse, or loss. The confidentiality of classified information, information deemed to be unclassified but sensitive in accordance with the Computer Security Act of 1987, and information subject to Privacy Act, privilege, proprietary, or other legislative or regulatory protections must be maintained.

Regardless of whether confidentiality is a factor, the integrity of DoD information must assured by protecting that information from illicit destruction or modification. Implicit in the notion of information integrity is the concept that, upon receipt of information, the recipient must be able to be sure from whom the information came and that it has not been modified in transit. Additionally, information must be available when and where needed to support analytic and decision-making processes. Objective No. 1 is, however, exclusively concerned with the issue of confidentiality; it is intended to help allocate information protection efforts.

[1] Approved by the Assistant Secretary on June 4, 1992; see Appendix A.

Statutes, Executive orders, and other applicable regulatory materials relevant to protection of information confidentiality have been assembled and reviewed. This report includes a history and analysis of selected statutory information protection mechanisms and a history of secrecy in the United States, from which it is clear that there is no unifying linkage among the statutes and Executive orders examined other than that provided by the FOIA. The report recommends establishing a blue-ribbon panel to provide overall advice and guidance to the Federal establishment with respect to information that may need protection as the geopolitical situation and our concept of what constitutes "national security" evolves.

This report further highlights the potential for improvements in security classification guidance and security awareness, education, and training. These areas are essential to a total quality approach to the protection of DoD information resources.

Responsibility for further action in response to Implementation Objective No. 1 of the CI&SCM Strategic Plan is assigned to the Defense Information Security Committee which will report progress to the ASD(C3I). This Committee, with assistance from the Acquisition Systems Protection Working Group, under the aegis of the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) (DASD(CI&SCM)), will make preparations for future work of the blue-ribbon panel by collecting and analyzing extant information protection studies and developing a synthesis of those for higher-level consideration. Additionally, it will continue to advise and assist the Information Systems Security Directorate, ODASD(CI&SCM) in the preparation of a new issue of DoD 5200.1-R, "Information Security Program Regulation" that will provide a unified policy document for protection of both classified and sensitive but unclassified information within the Department of Defense.

IMPLEMENTATION OBJECTIVE NO. 1

The following is taken from the June 4, 1992 CI&SCM Strategic Plan:

Prioritize which information needs protection, the threat through loss (and to whom), and the protection necessary.

THE STATUS: The development of guidance for determining the classification of information or designating unclassified information as sensitive is fragmented across numerous components and organizations. As a result, there is no standard process that would consider the value of the information to be protected to our policymakers and warfighters, or for determining the priority of the application of protective resources to classified or unclassified sensitive information. Moreover, DoD Components and organizations are attempting to define the threat to this information based on their own necessarily limited version of the national security environment. Further complicating this situation, information that is crucial to decision-making and warfighting (but that is not necessarily classified) increasingly resides on and is shared between automated information systems without requisite security considerations having been included in the design of the data networking process. Overall, this fragmentation of policy development has resulted in inadequate cost benefits analysis, uneven security levels, significant redundancy, cost escalation, and managerial inefficiencies. Fiscal responsibility dictates that we must carefully define what must be protected and concentrate our finite resources upon safeguarding our most important assets and information. This requires a fundamentally new way of thinking about the "security envelope" to be applied to our information and information systems in the post-Cold War period.

IMPLEMENTATION ACTION: By July 30, 1992, the ASD(C3I) will review the processes used for determining classification of information and designation of sensitive information, and develop an integrated approach -- to include establishing a senior review panel to provide cohesive and overall policy guidance -- that identifies, defines, and prioritizes the categories of information that require protection so that CI & SCM organizations can direct their shrinking resources to the most critical areas.

ACTION PLAN[2]

Determine the Threat Through Loss, and to Whom

- Provide a comprehensive analysis of the threat to national security information and to other DoD information

Prioritize Which Information Needs Protection

- Review the processes for determining classification of information and designation of sensitive information

- Develop guidance and standard processes for determining classification of information and designation of sensitive information

- Develop standard processes for prioritization of the application of protective resources to classified or unclassified sensitive information

- Develop an integrated approach

  - define the approach to be used in identifying and defining categories that need protection and prioritize the categories

  - establish a senior review panel to provide cohesive and overall policy guidance

Determine the Protection Necessary

- Direct CI&SCM resources to safeguarding the most critical assets and information

  - perform cost/benefit analyses in support of resource allocations

****** Near-Term Tasks ******

Review the processes for determining classification of information and designation of sensitive information

- Assemble relevant existing statutes, executive orders, and other applicable regulatory materials

- Review materials to determine the process currently in use

[2]This action plan was developed as a prelude to this report. It is the result of a decomposition of Implementation Objective No. 1 and is intended to ensure complete coverage of the objective.

- Document the current processes

Define the approach to be used in identifying/defining categories that need protection and prioritize the categories

- Develop an operational concept for applying internal CI&SCM resources to solving this problem

- Describe how the senior review panel contributes to the solution

- Document the approach

****** Longer-Term Tasks ******

Establish a senior review panel to provide cohesive and overall policy guidance

- Name an executive secretary

- Obtain staff support (internal and/or external to ODASD(CI&SCM))

- Identify potential members of the senior review panel

- Select an initial membership

- Solicit their participation (finalize draft letter for this purpose)

- Set up first meeting

Identify and define categories of information that need protection

- Assemble the results of previous efforts

- Prepare an input for the Senior Review Panel

- Action by the Senior Review Panel

Prioritize the categories

- Action by the Senior Review Panel

REVIEW AND ANALYSIS OF STATUTORY INFORMATION PROTECTION SYSTEMS

HISTORIES AND ANALYSIS

- Freedom of Information Act (FOIA). A people who mean to be their own governors must arm themselves with the power knowledge gives. James Madison wrote, "A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both."

The FOIA is based upon the presumption that the government and the information of government belong to the people. Consistent with this view is the notion that the proper function of the state in respect to government information is that of custodian in service to society. Yet such a presumption did not always prevail. Prior to the enactment of the FOIA in 1966, the burden was on the individual citizen to prove his right to look at government records. Moreover, there were no clearly delineated statutory guidelines to assist the individual seeking information and no judicial remedies for those wrongfully denied access. With the passage of the FOIA, however, the burden of proof was shifted from the individual to the government; the need to know standard was replaced by the right to know doctrine and the onus was upon the government to justify secrecy rather than the individual to obtain access. In addition, the legislation provided workable standards for what records should be open to public inspection and established judicial remedies for the aggrieved citizen. Above all, the statute made it clear that Federal agencies were hereinafter to provide the fullest possible disclosure of information to the public. In 1974, Congress enacted a series of refining amendments to the act which, among other things, encouraged even more disclosure than the original statute.

The legislative background of the FOIA is useful to understanding the key role FOIA enjoys in information protection systems. In 1958 Congress enacted a law, introduced in the House by Congressman John Moss and in the Senate by Senator Thomas Hennings, to correct the abuse of the Government's 180-year old housekeeping statute. The Moss-Hennings bill stated that the provisions of the 1789 statute, which permitted department heads to regulate the storage and use of government records, did not authorize withholding information or records from the public. This law produced some improvement with respect to the accessibility of Federal records, but the results were far from dramatic. Most agencies continued to operate in accordance with provisions of section 3 of the Administrative Procedure Act of 1946. This act was considered by many to encourage withholding rather than disclosure. Among other things, it authorized agencies to keep information secret "for good cause found," or where secrecy was in "the public interest," or where the information had a bearing on "any matter relating solely to the internal management of an agency." In addition, an agency was required to furnish information only to "persons properly and directly concerned."

It was not until 1966 that Congress enacted comprehensive legislation to deal with the problem of government secrecy. The FOIA of 1966 was milestone legislation that reversed long-standing government information practices. Enacted as an amendment to section 3 of the Administrative Procedure Act, it replaced the vague and general language of that law, and made it

clear that it was Congress' intent that any person should have access to identifiable records without having to demonstrate a need or even a reason. The burden of proof for withholding information, moreover, was placed on the government, as noted earlier. The act also broadened the scope of information available to the public and provided judicial remedies for those wrongfully denied information.

Despite the substantial shift in emphasis brought about by the 1966 act, some government agencies responded slowly and reluctantly to requests made under the law. In 1972, the House Foreign Operations and Government Information Subcommittee held 14 days of oversight hearings relating to the administration of the FOIA by Federal agencies and concluded that the "efficient operation of the Freedom of Information Act has been hindered by five years of foot-dragging by the Federal bureaucracy." As a result of its findings, the subcommittee proposed a number of procedural and substantive changes in the law. Two years later, Congress adopted amendments to the 1966 act. They became law over the veto of President Ford in February 1975.

The 1974 amendments were designed to speed and ease the process of obtaining access to government files. Among other things, they required agencies to publish comprehensive indexes for the administrative processing of requests for information, required that agency fees for locating and copying records be uniform and moderate, and shortened the Government's time for answering complaints brought into court. They also prohibited agencies from withholding entire documents, only parts of which were exempt, by requiring the release of nonexempt portions. In addition, they directed the courts to expedite consideration of FOIA cases, authorized judges to examine withheld documents and make an independent determination as to whether they should be released, and provided for the recovery of attorney fees by requesters who prevailed in litigation.

The 1986 amendments provided broader exemption protection for law enforcement information, plus new law enforcement record exclusions, and created a new fee and fee waiver structure. The fee provisions established a multi-tiered structure for the assessment of fees.

The FOIA applies only to documents held by the administrative agencies of the Executive branch of the Federal government. It does not apply to information maintained by the Legislative and Judicial branches. The Executive branch includes executive departments and offices, military departments, and independent regulatory agencies. All records in possession of these entities must be released upon request unless the information falls within one of the nine specific and narrowly drawn exemption categories.

Among other things, the FOIA grants public access to final opinions and orders of agencies, policy statements and interpretations not published in the Federal Register, administrative staff manuals, and government records that affect the public. Presidential papers have not been considered government records and have therefore not been required to be disclosed under the act.

The FOIA has become the cornerstone of many but not all information protection systems. As will be seen, other statutory protection systems rely on the provisions of the third exemption to mandatory disclosure, namely:

"specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."

Protecting unclassified information that is sensitive and thus important to the conduct of DoD business has the effect of making foreign intelligence services work harder to obtain that information. At the same time, it diminishes availability of foreign intelligence assets that can be targeted against classified DoD information. Protection of important, sensitive unclassified information is viable up to the time that a legal requirement for its release arises. Most often, this occurs through a request for the information being submitted pursuant to the FOIA. Essentially, any unclassified information must qualify under one or more of the eight non-security exemptions of the FOIA in order to be denied to a requester. Other copies of information may not be protected once it is released through the FOIA process.

The following explanation of the FOIA security and non-security exemptions is provided to bolster comprehension of other aspects of this report:

- Exemption (b)(1) applies to information which is currently and properly classified.

- Exemption (b)(2) applies to information which pertains to solely to the internal rules and practices of the agency; this exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document which, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.

- Exemption (b)(3) applies to information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

- Exemption (b)(4) applies to information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis which, if released, would result in competitive harm to the company.

- Exemption (b)(5) applies to inter- and intra-agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision making process, and contain subjective evaluations, opinions and recommendations.

- Exemption (b)(6) applies to information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

- Exemption (b)(7) applies to records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source, (e) disclose investigative techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.

- Exemption (b)(8) applies to certain records of agencies responsible for supervision of financial institutions.

- Exemption (b)(9) applies to geological and geophysical information.

The FOIA is the essential ingredient; it is the pivotal law that ultimately determines what governmental information can be protected from disclosure to the public. Information protection schemes that do not meet the tests of the FOIA fail when information protected by them is requested by an outside person who cites the FOIA.

- **Department of Defense Authorization Act, 1984**. A section (1217 of P.L. 98-94) of this Act provides the Secretary of Defense authority to withhold from public disclosure certain technical data with military or space application. In implementing this statutory authority to withhold information from public disclosure, the Department of Defense created a full fledged information dissemination system that now includes Canada. The DoD implementation is DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," which has been published in the Federal Register and is included in the appendices of this report.

The Department of Defense had sought legislation such as this for a number of years because of the exodus of valuable and sensitive but unclassified technology from the United States. A necessary consequence of the security classification process is the need to protect that which has been classified. Some technology and processes of military importance cannot be protected as classified information because they are not owned or controlled by the Department. Their unintended export often had adverse consequences. Further, the FOIA had been used to obtain militarily critical technical data that was not classified. Once released pursuant to the FOIA, such data were, technically, in the public domain and thus export control laws no longer applied.

DoD Directive 5230.25 implements 10 U.S.C. 140c, as added by - 1217 of P.L. 98-94, which states that the Secretary of Defense may withhold from public disclosure, notwithstanding other provisions of law, any technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be exported lawfully without an approval, authorization, or license under the export control laws, and provided further that the data are not subject to a general, unrestricted license or exemption in the Export Administration Regulations or International Traffic in Arms Regulations. The Department of Defense added one further test; the data also must be related to a militarily critical technology before they will be controlled under the Directive.

The implementing DoD Directive has two major features: it provides for the withholding of certain DoD technical data that meet the conditions noted above as well as provision of such data to requesters with legitimate requirements.

FOIA and other requests for export-controlled DoD technical data that are received from private individuals or enterprises are denied unless they are from "qualified U.S. contractors" (now "certified contractors" to recognize the inclusion of Canada in this program) within the meaning of the Directive. Becoming a "certified contractor" is accomplished by submission of DD Form 2345, "Militarily Critical Technical Data Agreement," to the Defense Logistics Agency's Defense Logistics Services Center. The certifications on this from are intended to allow technical data to be provided by the Department of Defense without making them available publicly, thus leaving the export control laws in force with respect to such data. The form asks for a brief business description to allow the Department of Defense to make the judgment that technical data requested in the future have a connection with the stated business of the requester. (The DD Form 2345 is included in the appendices.)

With few exceptions, "certified contractors" who request export-controlled DoD technical data for use in connection with their legitimate business can expect to receive that data from the Department of Defense, even when the business activity does not involve DoD or U.S. Government contracts.

Businesses have to establish themselves as "certified contractors" to receive DoD bid packages that contain technical data controlled under the Directive. Further, to the extent that export-controlled DoD technical data are involved, prospective prime contractors who are "certified contractors" are not able to share bid packages with prospective subcontractors unless the subcontractors are also "certified contractors."

Because of the nature of its business, the Defense Technical Information Center insists that its users also be "certified contractors."

Thus, it can be seen that the law implemented by this directive is given a different nature than its title suggests. To build an effective control system without at the same time crippling DoD activity, it became necessary to create a proactive technical data dissemination system.

- **Computer Security Act of 1987**. At the outset, Public Law 100-235 states that "The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use."

This law assigns to the National Institute of Standards and Technology (the National Bureau of Standards at the time of passage) responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal

computer systems, drawing on the technical advice and assistance of the National Security Agency. The law also requires establishment of security plans by all operators of Federal computer systems that contain sensitive information.

One of the significant features of the Computer Security Act of 1987 is its definition of sensitive information. The following is taken from the law:

"[T]he term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy...."

Thus, many DoD computer systems that do not process national security classified information are impacted by this law because of the broad definition of sensitive information.

- **Section 128 of title 10, United States Code**. Public Law 100-180 added this section to provide for the physical protection of special nuclear material by creating a limitation on the dissemination of certain unclassified information. A Friday, August 19, 1988 notice in the Federal Register stated that "In accordance with the foregoing authority, the Deputy Secretary of Defense hereby prohibits the unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material. This prohibition shall be applied by Department of Defense personnel to prohibit the dissemination of any such information only if and to the extent that it is determined that unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of: illegal production of nuclear weapons; or theft, diversion, or sabotage of special nuclear material, equipment, or facilities."

The above is the forerunner of DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)" which has a counterpart within the Department of Energy. The Directive provides a full compliment of safeguarding procedures for UCNI including the guidance that the Department's FOIA regulation applies to requests for public release of UCNI. Information that qualifies as DoD UCNI, under 10 U.S.C. 128, is exempt from mandatory disclosure under 5 U.S.C. 552 which is the FOIA. Consequently, requests for the public release of DoD UCNI shall be denied under section 552(b)(3) of the FOIA, citing 10 U.S.C. 128 as the authority.

- **National Security Agency Act of 1959**. Sect. 6 of Public Law 86-36, which provides certain administrative authorities for the National Security Agency, effectively says that the Director of the National Security Agency does not have to publish information about the Agency's missions, people, or organizations. It is deemed to be a law within the meaning of section 552(b)(3) of the FOIA. A copy of this Act is included in the appendices.

- **Central Intelligence Agency Act of 1949**. This and related laws (e.g., the "espionage statutes") provide for the protection of intelligence sources and methods, including the identities of certain U.S. undercover intelligence officers, agents, informants, and sources.

- **Atomic Energy Act of 1954**. This statute, as amended over the years, creates the category of classified information known as Restricted Data. It is, therefore, unique in this collection of statutes in that none of the others classify information and most do not even deal with classified information.

There are many differences between the classification of national security information (NSI) and Restricted Data / Formerly Restricted Data (RD / FRD). RD is information concerning the design, production, and use of special nuclear material. As indicated, there are distinct legal origins for the two systems. NSI is classified pursuant to authority that flows from Presidential executive orders. RD classification is based on the Atomic Energy Act. RD is "born classified" and it takes a great deal of effort to rescind the RD classification. Indeed, only the Department of Energy (DoE) has the requisite authority while DoE and DoD must agree on the declassification of FRD. NSI is a broad category of information while RD is narrow and focused; NSI is owned by or controlled by the government while RD may be private or even foreign information. Other contrasts abound. The original classification of NSI is allowed by the current Executive order whereas the original classification of RD is done by the Atomic Energy Act.

The Atomic Energy Act is a law within the meaning of section 552(b)(3) of the FOIA.

- **Other Laws**. Other laws that limit distribution or mandate confidentiality are worth mentioning. One is the Privacy Act relating to personal information. It is a law within the meaning of section 552(b)(3) of the FOIA. From the viewpoint of a foreign person, U.S. export control laws are viewed as regulating access to technical data although these laws do qualify under section 552(b)(3) of the FOIA.

COMPARISON OF STATUTES

An overwhelming conclusion that emerges from these reviews is that there is no unifying linkage among the statutes (and Executive orders examined later on in this report) other than that provided by the FOIA. Another conclusion that emerges from this analysis is the fact that individual laws addressing control of unclassified information by the Department of Defense (or by other departments or agencies in the Federal bureaucracy) were established to deal with particular issues of a given time. There is no single logic thread connecting the statutes. Barriers to effective information protection arise from these circumstances. The FOIA does provide connections to other qualifying statutes as noted above but these connections do not provide a unified approach to regulating access.

The statutes cited in this report treat differing subject matter areas and differing sensitivity scales. These range from purely personal information of employees to the identification of clandestine intelligence agents to the design of nuclear weapons.

To be effective in regulating access, at least in the context of FOIA requests and litigation, information control laws must meet one or more of the tests set forth in 5 U.S.C. 552(b)(3) or any of the other FOIA exemptions. 5 U.S.C. 552(b)(3) is the FOIA exemption that in effect specifies that the Federal establishment may withhold what another law says can be withheld. This suggests a possible departure point for a future effort to codify information protection laws, to include creation of a statutory basis for the security classification system should one be desired.

This latter point raises legal difficulties with respect to the separation of powers concept. The President must have the flexibility necessary to discharge his Constitutional duties. Further discussion of this topic is contained in the history of the classification system that follows. It is a topic that requires close examination by any blue-ribbon committee created as a consequence of Implementation Objective No. 1.

IDENTIFICATION PROCESSES

This section highlights the differences between the identification of classified information and the general lack of mature identification processes for unclassified but sensitive information that is protected by statute. Extant identification processes are largely -- but not entirely -- developments of departmental or agency implementations of statutes. Perhaps most notable in this regard is the identification of information that may be withheld from disclosure to the public pursuant to the FOIA. The Department of Defense utilizes the label "For Official Use Only" while the Department of State uses the term "Limited Official Use." The Department of Energy uses "Official Use Only." The Central Intelligence Agency utilizes "For Official Use Only" for some information. An Executive order implementing the FOIA could standardize these labels and associated protection requirements. Standardization should lead to both quality and productivity increases with a resultant decrease in costs.

At the present time there is not an established system for identifying "sensitive information" within the context of the Computer Security Act of 1987. Treatment of all Federal information as "Sensitive" in this context would create enormous burdens on available protective systems and resources. Protection in this context must encompass confidentiality, integrity, and availability of sensitive data. Additionally, computers must be understood as including their communication systems. Thus, it is essential that a rational mechanism to identify that which is "sensitive" be established and implemented. Though any protection mechanism must encompass confidentiality, integrity, and availability of data, it should focus on simplicity and economy. That will reduce implementation costs and promote uniformity.

Ideally, the various identification labels for unclassified information that have been devised to date would be distilled to one or two. An impediment to reaching this goal is the presence of some identification labels in legislation. "Unclassified Controlled Nuclear Information" is a prime example. Any attempt to codify present statutory provisions should address this facet of the identification process.

The identification of classified information is a very mature art form and perhaps the systems in use in the field of sensitive, unclassified information need not be so sophisticated. Nonetheless, an integrated approach would have clear advantages vis-à-vis the present situation. Quality of implementation would improve while cost of education and implementation would decline.

REVIEW AND ANALYSIS OF SECURITY CLASSIFICATION SYSTEM

HISTORY[3]

World War II (W.W.II) had a major effect on the classification and control of information in the United States. It will be seen that W.W.II is the turning point in information protection in the United States. Throughout most of our country's early history until W.W.II, the government's concern with protection of information had been mostly limited to a relatively small amount of information closely related to military and diplomatic matters. The breadth and depth of security classification of information in the United States significantly expanded during and after W.W.II. For example, not until W.W.II was secrecy widely imposed by the government on scientific and technical information. Since W.W.II it has not been unusual for scientific and technical information to be classified by the government.

The first Executive order (EO) dealing with classification was issued in 1940, shortly after W.W.II began in Europe. The first statute dealing with information classification, the Atomic Energy Act, was enacted in 1946 shortly after W.W.II had ended. That statute defines "Restricted Data."

Restrictions on the dissemination of information related to the military and its operations have existed since the beginnings of our country. During the Revolutionary War, the 1775 Articles of War prohibited unauthorized correspondence by soldiers of the Continental Army with an enemy. Those wartime regulations were directed primarily to military personnel and were limited to the control of military information.

Some of the first instances of "civilian" governmental control of information in the "United States" were by the Continental Congress (1774-1789). Members of the First Continental Congress (1774) were requested to keep the proceedings secret, in accordance with the following resolution which was passed by the Congress on September 6, 1774, its second day of business:

> Resolved, That the doors be kept shut during the time of business, and that the members consider themselves under the strongest obligations of honour, to keep the proceedings secret, until [sic] the majority shall direct them to be made public.

However, at the end of the First Continental Congress its proceedings were ordered to be published.

The Second Continental Congress also requested its members to keep the proceedings secret. A resolution nearly identical to that adopted by the First Continental Congress was passed on May 11, 1775, the second day of business of the Second Continental Congress. A more detailed resolution to that effect was passed on November 9, 1775, as follows:

---

[3] "Security Classification of Information," Volume 1, Introduction, History, and Adverse Impacts," K/CG-1077/V1, Arvin S. Quist

> On motion made, Resolved, That every member of this Congress considers himself under the ties of virtue, honor and love of his country not to divulge directly or indirectly any matter or thing agitated or debated in Congress before the same shall have been determined, without leave of the Congress; nor any matter or thing determined in Congress which a majority of the Congress shall order to be kept secret and that if any member shall violate this agreement he shall be expelled from this Congress and deemed an enemy to the liberties of America and liable to be treated as such and that every member signify his consent to this agreement by signing the same.

This Congress also, at an early date (July 25, 1775), authorized a committee to "revise" the "Journals of the Congress, and prepare it for the press." Apparently, not all of those proceedings were initially made public, since in November 1775 the Congress authorized further publication of its proceedings and asked the committee responsible for this matter "to examine whether it will be proper yet to publish any of those parts omitted in the journal of the last session."

The Second Continental Congress established two "secret" committees, the "Secret Committee" and the "Committee of Secret Correspondence." The Secret Committee was established on September 18, 1775, and dealt mainly with the purchase of weapons, ships, and other war materials - "national defense" matters. The Committee of Secret Correspondence was established on November 29, 1775, for the purpose of corresponding with "friends" in other parts of the world - "foreign relations" matters. This committee later became known as the "Committee for Foreign Affairs." Thus at an early date the Second Continental Congress had established committees dealing with national defense and foreign relations and had acknowledged the importance of secrecy in certain military and diplomatic activities. Those activities, usually the responsibility of a government's executive branch, were the responsibility of the Continental Congress because at that time there was no executive branch of our government.

There are other examples of secrecy in our early government. However, the U.S. Constitution mentions secrecy only once. Article I, Section 5, authorized the House and Senate to publish the journal of their proceedings, "excepting such Parts as may in their Judgment require Secrecy." This section was derived from a similar provision in the Articles of Confederation, as mentioned earlier.

Since our nation was founded, Presidents have used their implied Constitutional authority to control the dissemination of information related to national defense and foreign relations. The Supreme Court and Congress have acknowledged this implied authority as necessary for Presidents to execute their responsibilities under Article II, Section 2, of the Constitution as Commander-in-Chief of the nation's armed forces and as the Chief Executive responsible for the conduct of foreign relations. An early instance of a President's use of this authority to restrict the dissemination of information occurred in January 1790, when President Washington transmitted information about negotiations with some Southern tribes of Indians to Congress as a "confidential communication." Later that year the President sent to the Senate a proposed secret article to a treaty with the Creek Indian nation. Subsequently, it was not unusual for certain military or diplomatic communications to be designated as "confidential."

Between the Revolutionary War and the Civil War, certain governmental documents were given special markings to aid in restricting their distribution. Governmental use of the terms "Secret," "Confidential," and "Private" has been traced back to the War of 1812.

The new developments in weapons technology in the mid-19th century were initially not especially protected. Great Britain was the first nation to recognize the need to restrict access to information concerning its naval mines; Great Britain consequently applied restrictive defense markings to that information.

In the 1880s Britain further recognized the need to protect weapons technology. In awarding contracts to produce a new design of torpedo, the British Admiralty awarded separate contracts, to different companies, for the different torpedo components. The rationale was that this separation (that is, compartmentation) would prevent any single nongovernmental employee from knowing all the information required to build the torpedo. The chance that a foreign government could obtain this information was thereby diminished.

After the Civil War, the U.S. Army and Navy initiated some activities that recognized the importance of military information ("intelligence"). Military attaches were assigned to many U.S. embassies. Formal Naval and Army intelligence branches were established in 1882 and 1885, respectively.

The first peacetime U.S. governmental directives that were concerned with the protection of information were issued in 1869. In that year the Army issued an order restricting the availability of certain information on Army forts. The regulation prohibited photographs or other views of those forts except with the permission of the War Department.

In 1898 Congress enacted a statute that established a penalty for damaging fortifications or harbor-defense systems, or interfering with their operation, or violating any War Department regulations made for the protection of such systems. The penalty was a fine ($100-$5000) or imprisonment (not more than 5 years) or both. Thus, penalties for violating the previously mentioned Army regulation protecting information on forts and harbor-defense facilities were now applicable to civilians as well as to military personnel.

In 1912 the War Department provided regulations for marking and safeguarding certain documents, mostly concerning coastal defenses and other fortifications, as "Confidential." Documents so marked were to be kept under lock, to be uniquely numbered, to be periodically inventoried, and not to be copied except by the issuing office. These regulations possibly reflect the earliest use of a numbering system and periodic inventory requirements for classified documents.

After the April 1917 entry of the United States into World War I and the arrival of the first American troops in France, the American Expeditionary Force promulgated regulations to protect official information. Those regulations, issued in November 1917, were patterned after French and British classification procedures. (The French were said to have used "Secret" and "Confidential" terminology; the British also used "For Official Use Only.") Shortly thereafter, in

December 1917, the War Department adopted similar regulations to be applicable throughout the Army. Those regulations established three markings as follows:

Secret - limited the use or sight of a document to the officer to whom it was delivered and, when necessary, to a confidential clerk;

Confidential - restricted the document for use and knowledge to a necessary minimum number of persons;

For Official Use Only - indicated that the document was for official circulation only and was not intended for the public or the press. (The American Expeditionary Force used the terminology "For Official Circulation Only.")

From the end of World War I until nearly the beginning of W.W.II, the military regulations for classifying information remained much the same as those issued in 1917. One major change occurred in Army regulations in 1921. This change provided guidance concerning identification of the information to be protected, rather than concerning who was allowed to see the information. The "Secret" marking was to be used for information "of great importance and when the safeguarding of that information from actual or potential enemies is of prime necessity." "Confidential" was to be used for information "of less importance and of less secret nature than one requiring the mark of 'Secret.'" Also included in the 1921 regulations were requirements to indicate the name and authority of the classifying officer and the date of classification. Instructions provided for the possibility of canceling the classification marking at a later time.

In 1935 the Army introduced a fourth marking, "Restricted," which was designed to protect "research work or the design, development, test, production, or use of a unit of military equipment or a component thereof which it is designed to keep secret."

In February 1936 the Army redefined "Secret," "Confidential," and "Restricted" for use in marking documents under its purview and discontinued the use of "For Official Use Only." Information falling within the latter category was incorporated into the new "Restricted" definition. The new definitions broadened the types of classifiable information to include non-defense information. Protecting "national security" was mentioned as a reason for classifying information. By implication, foreign policy information seemed to be included within the new definitions. The "Secret" designation was to be applied to information whose disclosure "might endanger the national security, or cause serious injury to the interests or prestige of the Nation, an individual, or any government activity, or be of great advantage to a foreign nation." Throughout this time the Navy's classification regulations were similar to the Army's. Neither service's regulations applied to information or materials not under their control, nor did they apply to nonmilitary personnel. However, the scope of those regulations had expanded significantly beyond information on Army fortifications as first regulated in 1869.

W.W.II is the time frame for the beginning of classification systems under Presidential Executive orders that are familiar today. Although Congress has not explicitly authorized an Executive order dealing with classification of information, it has given the classification system

implicit approval via statutes. Under Sect. 552(b)(1) of the Freedom of Information Act (FOIA), Congress has exempted from disclosure documents that have been properly classified under an Executive order. Under the Internal Security Act of 1950, Congress has prohibited government employees from giving information classified by the President (or under his direction) to foreign agents. The Computer Security Act of 1987 (Public Law 100-235) recognizes the classification system also. Its definition of "sensitive" information excludes information that has been authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy.

The first Executive order dealing with classification was Executive Order 8381, "Defining Certain Vital Military and Naval Installations and Equipment," issued on March 22, 1940 by President Franklin D. Roosevelt. The main effect of this order was to establish Presidential approval of what the Army and Navy were already doing. It also gave governmental civilian employees the authority to classify information, since it provides that information could be classified "with the approval or at the direction of the President in addition to being classified by authority of the Secretary of War or the Secretary of the Navy." Until this time, military personnel had been the only recipients of governmental classification directives. Three classifications were provided: Secret, Confidential, and Restricted.

The second Executive order dealing with classification of information was Executive Order 10104, "Defining Certain Vital Military and Naval Installations and Equipment as Requiring Protection Against the General Dissemination of Information Relative Thereto." It was issued by President Truman on February 1, 1950. It included the three classifications of the first Executive order and added a fourth classification of Top Secret.

The first two Executive orders on classification were based on a 1938 defense installation statute. Orders from this point to the present day do not cite such a specific authority, relying instead on authority vested in me (the President) by the Constitution and laws.

The first of these Executive orders was Executive Order 10290 that provided a comprehensive system for identifying and protecting information "the safeguarding of which is necessary in order to protect the security of the United States." Information was classified under this order at one of the four established levels and also was identified as "Security Information." Terms were defined and regulations were included to classify, upgrade, downgrade, declassify, disseminate, and handle (mark, transmit, store, and destroy) classified security information. This and the orders that followed resemble the current Executive order to that extent.

COMPARISON OF CONTEMPORARY EXECUTIVE ORDERS

The following is a comparison of the major classification features of Executive Orders 10290 through the present day.

TIME FRAME - 17 September 1951 to 14 December 1953 (Truman's E.O.)

Executive Order 10290, "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States"

Executive Order 10290 provided for a four-tier security classification system, namely, Restricted, Confidential, Secret, and Top Secret. The damage test did not exist as such. Other and different criteria for assignment of each classification were:

- Restricted - shall be applied to information having such bearing upon national security as to require protection against unauthorized use or disclosure, particularly information which should be limited to official use.

- Confidential - shall be given only to information which requires careful protection in order to prevent disclosures which might harm national security.

- Secret - shall be given only to information which requires extraordinary protection in the interest of national security.

- Top Secret - unauthorized disclosure could result in exceptionally grave danger to the national security.

Provisions were made for downgrading and declassification, either automatically or non-automatically. Markings instructing downgrading and/or declassification could be placed on documents by the classifying official.

TIME FRAME - 15 December 1953 to 31 May 1972 (Eisenhower's E.O.)

Executive Order 10501, "Safeguarding Official Information in the Interests of the Defense of the United States," as amended several times including the significant declassification amendments of Executive Order 10964, 20 September 1961.

Executive Order 10501 provided for a three-tier security classification system, namely, Confidential, Secret, and Top Secret. The damage tests for assignment of each classification were:

- Confidential - unauthorized disclosure could be prejudicial to the defense interests of the nation.

- Secret - unauthorized disclosure could result in serious damage to the Nation.

- Top Secret - unauthorized disclosure could result in exceptionally grave damage to the Nation.

The downgrading and declassification system from 20 September 1961 was as follows:

- Group 1. Information or material originated by foreign governments or international organizations and over which the United States Government has no jurisdiction, information or material provided for by statutes such as the Atomic Energy Act, and information or material requiring special handling, such as intelligence and cryptography. This information and material is excluded from automatic downgrading or declassification.

- Group 2. Extremely sensitive information or material which the head of the agency or his designees exempt, on an individual basis, from automatic downgrading or declassification.

- Group 3. Information or material which warrants some degree of classification for an indefinite period. Such information or material shall become automatically downgraded at 12-year intervals until the lowest classification is reached, but shall not become automatically declassified.

- Group 4. Information or material which does not qualify for, or is not assigned to, one of the first three groups. Such information or material shall become automatically downgraded at 3-year intervals until the lowest classification is reached, and shall be automatically declassified 12 years after date of issuance.

TIME FRAME - 1 June 1972 to 30 November 1978 (Nixon's E.O.)

Executive Order 11652, "Classification and Declassification of National Security Information and Material."

Executive Order 11652 provided for a three-tier security classification system, namely, Confidential, Secret, and Top Secret. The damage tests for assignment of each classification were:

- Confidential - unauthorized disclosure could reasonably be expected to cause damage to the national security.

- Secret - unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

- Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

The downgrading and declassification system under Executive Order 11652 was as follows:

- General Declassification Schedule:

- Top Secret - Information or material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

- Secret - Information or material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar following the year in which it was originated.

- Confidential - Information or material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

- Exemptions from the General Declassification Schedule:

Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official authorized to originally classify information or material "Top Secret" may exempt from the General Declassification Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

- Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

- Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

- Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

- Classified information or material the disclosure of which would place a person in immediate jeopardy.

TIME FRAME - 1 December 1978 to 31 July 1982 (Carter's E.O.)

Executive Order 12065, "Classification and Declassification of National Security Information and Material."

Executive Order 12065 provided for a three-tier security classification system, namely, Confidential, Secret, and Top Secret. The damage tests for assignment of each classification were:

- Confidential - unauthorized disclosure could reasonably be expected to cause identifiable damage to the national security.

- Secret - unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

- Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

The declassification system under Executive Order 12065 was as follows:

- At the time of original classification each original classification authority shall set a date or event for automatic declassification no more than 6 years later.

- Only officials with Top Secret classification authority and [certain] agency heads may classify information for more than 6 years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than 20 years after original classification, except that for foreign government information the date or event may be up to 30 years after original classification.

TIME FRAME - 1 August 1982 to the Present (Reagan's E.O.)

Executive Order 12356, "National Security Information"

Executive Order 12356 provided for a three-tier security classification system, namely, Confidential, Secret, and Top Secret. The damage tests for assignment of each classification were:

- Confidential - unauthorized disclosure could reasonably be expected to cause damage to the national security.

- Secret - unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

- Top Secret - unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

The declassification system under Executive Order 12356 is as follows:

- Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. [When a declassification date or event cannot be determined, the information is marked with the notation "Originating Agency's Determination Required" or "OADR."]

IDENTIFICATION PROCESSES

ORIGINAL CLASSIFICATION POLICY

Original classification is an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. Original classification authority is delegated in writing.

Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, "National Security Information" provides the only basis for classifying information. The only reason for security classification of information is to protect the national security which is defined as the national defense and foreign relations of the United States. This policy is implemented within the Department of Defense by DoD 5200.1-R, "Information Security Program Regulation."

An original decision to classify shall be made only by an official with that authority when, first, it is determined that the information in question is within one of several categories that are classifiable, and, second, a separate determination is made that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

If both of the foregoing determinations are affirmative, DoD information requiring protection against unauthorized disclosure, or uncontrolled dissemination, shall be classified at one of three levels, namely: Top Secret, Secret, or Confidential. The Top Secret designation shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. The Secret designation shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. And the Confidential designation shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Examples of exceptionally grave damage to the national security, the test for application of the Top Secret classification, include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, compromise of national-level cryptographic systems, exposure of some intelligence sources or methods, and substantial disruption of the capability of the National Command Authority to function in times of peace or crisis. Examples of serious damage and damage to national security are progressively less calamitous.

Original classification authorities shall set a date or event, consistent with national security, on which automatic declassification should occur. They may provide for indefinite duration of classification only when this cannot be done.

Once the classification decision is made, the original classifier incurs the responsibility for communicating that decision to others who have need for the classified information through appropriate markings or other guidance. This responsibility to provide security classification guidance extends to industry when classified contracting is involved.

Original classification authority flows from the President of the United States through Executive Order 12356 to the heads of various Executive branch departments of agencies. The President has conferred original Top Secret classification authority upon four officials within the Department. They are the Secretary of Defense and the Secretaries of the Military Departments. These officials may delegate this authority to their subordinates.

Extant DoD security classification policy requires that classification guides be maintained in phase with project milestones to the degree practicable. This concept has been reinforced recently by actions of the Acquisition Systems Working Group that mandates that protection plans be developed along project milestone lines. Classification guides are to be understood as the written record of a decision or series of decisions to classify information. Classification guides shall:

- Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly;

- State which of the classification designation (that is, Top Secret, or Confidential) applies to each element or category of information;

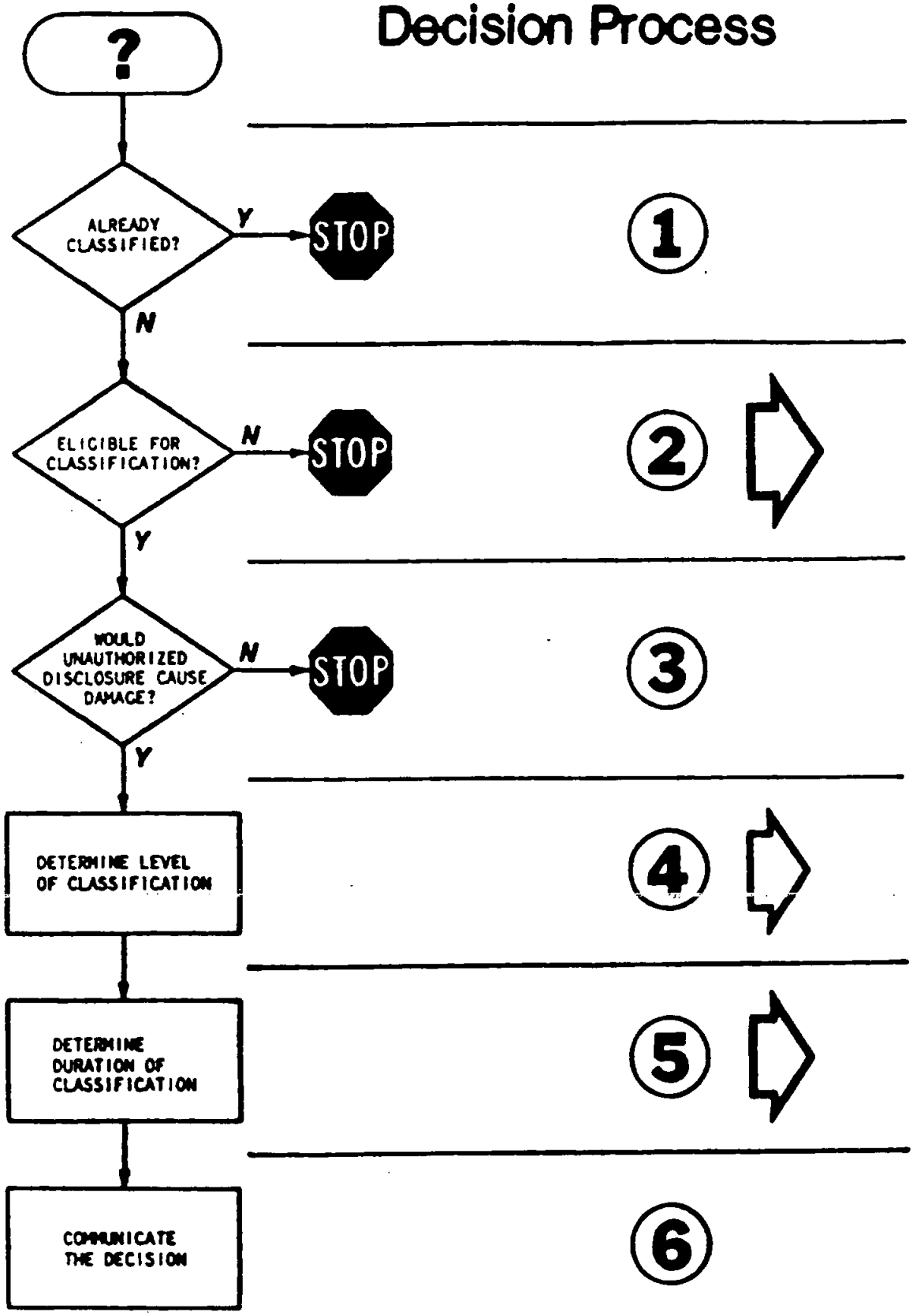
- State declassification instruction for each element or category of information in terms of a period of time, the occurrence of an event, or a notation that the information shall not be declassified automatically without approval of the originating agency; and

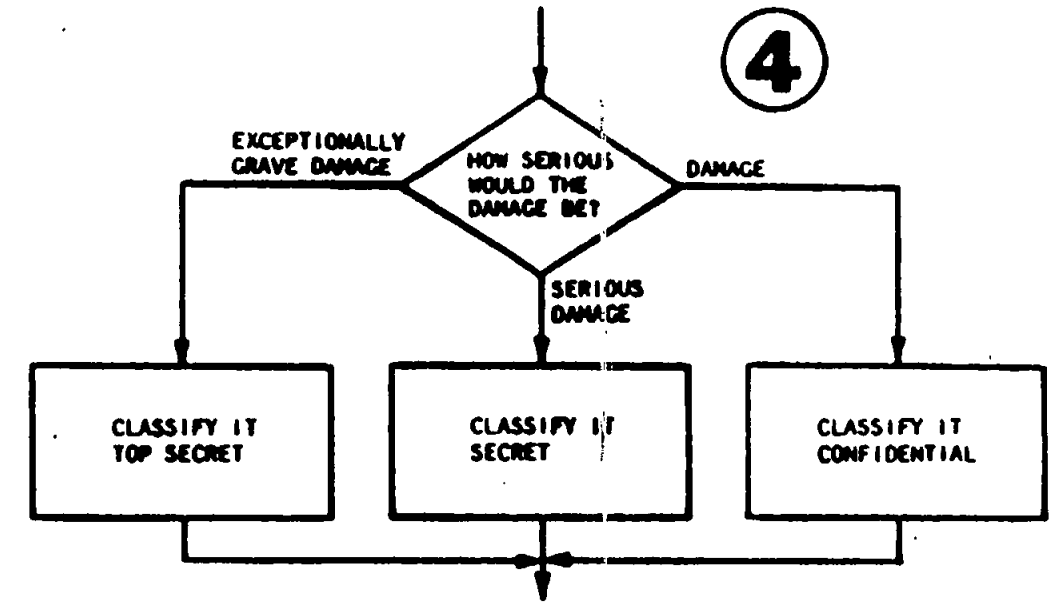
- State any special public release procedures and foreign disclosure considerations.

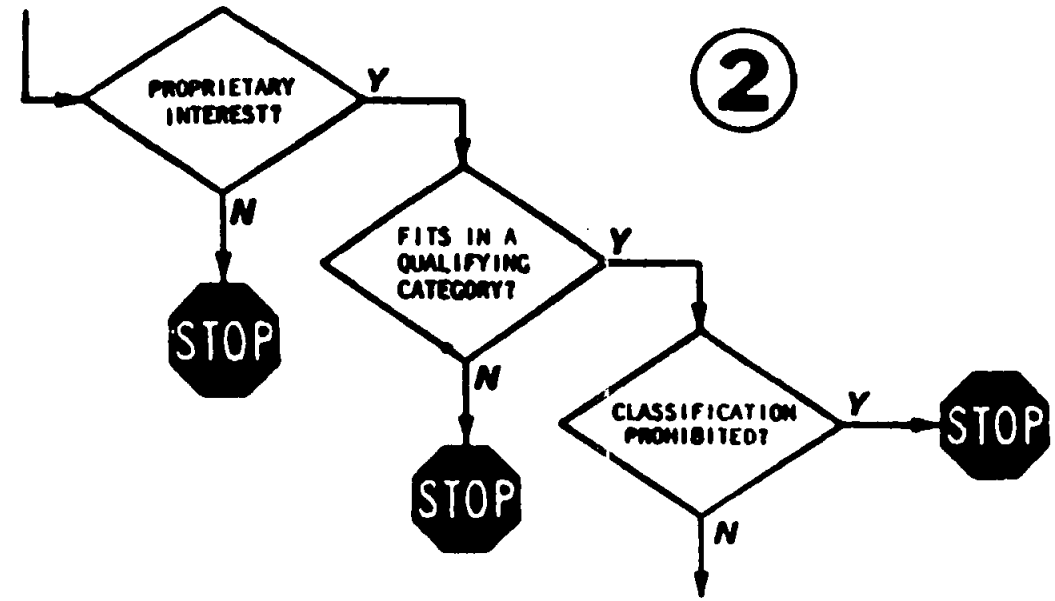
Security classification cannot be used for the sole purpose of concealing violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization, or agency, or to restrain competition.

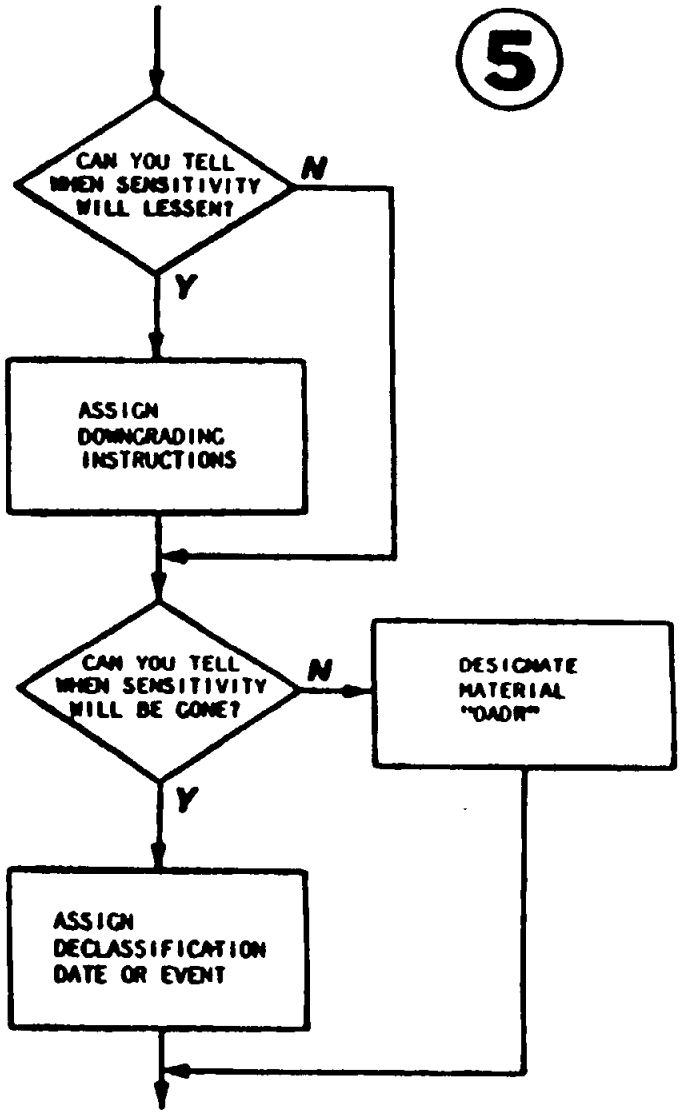
The flow chart that appears on the next two pages illustrates the original security classification process.

The Original Classification Decision Process




4
HOW SERIOUS WOULD THE DAMAGE BE?
EXCEPTIONALLY GRAVE DAMAGE
SERIOUS DAMAGE
DAMAGE
CLASSIFY IT TOP SECRET
CLASSIFY IT SECRET
CLASSIFY IT CONFIDENTIAL


2
PROPRIETARY INTEREST?
Y
N
STOP
FITS IN A QUALIFYING CATEGORY?
Y
N
STOP
CLASSIFICATION PROHIBITED?
Y
N
STOP


5
CAN YOU TELL WHEN SENSITIVITY WILL LESSEN?
N
Y
ASSIGN DOWNGRADING INSTRUCTIONS
CAN YOU TELL WHEN SENSITIVITY WILL BE GONE?
N
DESIGNATE MATERIAL "OADR"
Y
ASSIGN DECLASSIFICATION DATE OR EVENT

ORIGINAL CLASSIFICATION PRACTICE

Anecdotal evidence suggests that original classification practice does not always match classification policy.

In a Department as large as the Department of Defense, there is need to improve constantly the implementation of security classification rules. This is abundantly clear when the constant turn-over of supporting staff and officials who occupy positions involving original classification authority, and the press of business, are considered.

Implementation Objective No. 1 recognizes the central role of the original classifier. The decision by that person to protect information within his or her domain is the one that triggers implementation of other security disciplines. This trigger mechanism inherently is part of the process of classification of information. A bad decision to protect information has the same consequences as does a proper decision. That is, both lead to the safeguarding of information at some expense to the government and its taxpayers. Original classification practice does not support the quality judgments that should lead to increased productivity and, ultimately, lower costs for the security of information within the Department of Defense.

In an effort to help others foresee problems that may arise as a consequence of their original classification decisions, and to achieve constancy of purpose, the Department of Defense developed and published in 1976 a "DoD Index of Security Classification Guides" for use by its classifiers and others with an information protection responsibility. The Index provides opportunity for classifiers in one part of the Department of Defense to learn of the classification decisions made by others. Constancy of classification action would result if all classifiers were in a position to know of similar action by peers. To a degree, the Index achieves this purpose but it can be crafted into a more useful tool. An expanded version of the Index could bring more structure and uniformity to the classification process within the Department of Defense.

Seemingly, the original classification process is given little serious attention in some environments of the Department. Practice does not fit policy when the secretary to a director is told to take care of classifying the document just signed.

Classification practice in many situations is by rote. "It always has been classified and this is too" is a refrain heard too often. A mistake made once is repeated with no conscious effort to understand why the information needs protection. And consequences of improper and unnecessary protection of information are not evaluated. Also, the original decision to protect may have been proper at the time it was made but circumstances surrounding the decision changed without an accompanying reevaluation of classification. The "by rote" syndrome is one that absolutely eliminates any chance of building quality into the classification process.

Whether by rote or otherwise, classification decisions are made without full consideration of the status of like information on a world-wide basis. Full utilization scientific, technical,

intelligence, and public affairs resources would eliminate barriers to quality classification decisions. That in turn would lead to increased productivity and ultimately to reduced costs.

Some bureaucrats engage in "prestige classification" - the practice of classifying at the highest level, or adding compartmentation symbols to the classification - as a means of assigning importance to information. This practice must be eliminated.

There are indications that some information is classified because it may be useful to another nation. While the motivation for such classification is understood, especially when viewed from the light of the Cold War, it is still incorrect classification. This suggests that not enough has been done to provide the classifier the tools needed for a quality job. Security awareness, education, and training investments for classifiers should produce a significant return on investment by decreasing overall costs of classification and preventing loss of information of value.

DERIVATIVE CLASSIFICATION POLICY

Derivative classification is a determination that information is in substance the same as information that is currently classified. The derivative classification process includes application of the same classification markings to the newly created material. Derivative classification is a responsibility (as contrasted to authority in the context of original classification authority) of those who work with classified information.

Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings in accordance with guidance from an original classification authority. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Persons who apply such derivative classification markings must:

- Respect original classification decisions;

- Verify the information's current level of classification as far as practicable before applying the markings; and

- Carry forward to any newly created documents the assigned dates or events for declassification and any additional authorized markings.

The Department of Defense and other Federal agencies have in place derivative classification policy as described above. From the vantage point of the Executive order and implementing directives, other approaches are possible. The Department of Energy treats derivative classification in much the same fashion as the Department of Defense treats original classification. That is, derivative classifiers are designated as such in writing by DoE management.

Providing for the written designation of derivative classifiers, and thus excluding all others from the process, should be explored. There are pros and cons to this approach, however. On the plus side of the equation, it should be expected that the quality of implementation of the derivative classification process would improve. Education and training could be targeted more precisely. On the other side of the equation is the fact that new bureaucratic structures would have to be built and operated with already scarce resources.

DERIVATIVE CLASSIFICATION PRACTICE

Derivative classification accounts for the vast majority (98%) of classification determinations made by DoD officials. It works reasonably when portion markings are present on the source documentation or when written security classification guidance is explicit enough to remove discretion from the process.

Derivative classification based on source documentation is commonplace in administrative business settings that often lack written classification guides. This occurs because of the difficulty in drafting guides to cover the wide array of national security-related situations that may arise in a Pentagon staff office, for example. This suggests there is a possibility to provide additional tools (classification guides) for derivative classifiers that would cover missions as opposed to the more common situation of classification guides for systems. Overall efficiency of staff operations could improve in many circumstances.

Source document derivative classification, that is, taking information and its classification from one document for use in another, does have strengths and weaknesses. The paragraph is generally accepted as the smallest portion of a document that is separately identified with classification markings ((C), (S), (TS) or (U) to indicate unclassified). The strength comes from the idea that the secret may be contained in a single sentence. The portion marking protects not only that sentence but the sentences that surround it. Thus, there is less likelihood of disclosing the secret through association with other unprotected information. On the negative side, using the same illustration, the unclassified information surrounding the secret sentence gets a classification label when it is used elsewhere. The derivative classifier is not empowered to do otherwise and thus the total amount of information protected by security classification may grow unnecessarily. As information is recycled more often, unnecessary classification becomes worse. Costs increase while quality (properly classified information) decreases.

The importance of the preceding paragraph cannot be overstated. Except for chain-of-command situations, a derivative classifier has no authority to and may not make a determination that information is to be handled in a manner other than as marked. Such authority inherently is that of the original classification authority. The derivative classifier who changes the decision of another brings chaos to the classification system. This is occurs because information is protected and not protected at the same time or information is protected simultaneously at differing classifications. Even when a derivative classifier exercises good common sense, and treats "obviously" unclassified information within a Secret classified paragraph as unclassified, he or she is acting without authority and will, sooner or later, make mistakes because he or she does not know better than the original classifier.

Derivative classification based on classification guides tends to be more common in offices responsible for high-technology systems such as state-of-the-art missiles. A classification guide acts as a written record of a series of classification decisions by an original classification authority (in charge of missiles, to continue the example). If it correctly describes information to be classified, and does so with precision, a potential exists that only that information requiring

protection in the national interest will be classified by derivative classifiers. This is only a potential because the classification guide must be available, must be read, and must be understood by those who need it.

Managers of programs with national security information should want to promulgate the best guidance possible. The investment of time to do the guide right should be expected to create program savings downstream while assuring the security of the program. Program savings should accrue because there would be less or no need to correct mistakes. The percentage of productive time spent to accomplish program activities increases.

At the time of initial preparation of classification guides, program managers need to provide guidance based on anticipated acquisition or other milestones in the program. This has been addressed recently (in the Acquisition Systems Protection Master Plan) but the regulatory guidance to that effect -- which has been in place since 1972 -- often is ignored. The consequences may be unnecessarily long protection of information at too high a level.

DEFINITION OF APPROACH TO BE USED IN IDENTIFYING AND PRIORITIZING CATEGORIES OF INFORMATION NEEDING PROTECTION

In all likelihood, there is no single best answer to achieving the stated or any implicit goals of Implementation Objective No. 1 of the CI&SCM Strategic Plan. Thus, there should be flexibility and willingness to make adjustments to the approach recommended by this report. Any adjustments ought to be based on experience gained in the course of pursuing the goal.

Much work has been done in the area of identifying that which needs protection. Identification of the work accomplished to date should be prerequisite to further efforts in identifying, defining, and prioritizing the categories of information that require protection so that CI&SCM organizations can direct shrinking resources to the most critical areas.

The Defense Information Security Committee (DISC) is chartered by Section 5, Chapter XIII, DoD 5200.1-R, "Information Security Program Regulation" to assist in the formulation of DoD Information Security Program policy and procedures. The DISC is comprised of senior security representatives of the major DoD Components. The DISC is at the disposal of the ASD(C3I) and should be tasked to continue the process initiated with the June 4, 1992 approval of the CI&SCM Strategic Plan.

The Acquisition Systems Protection Working Group (ASPWG) should contribute to the process. It has developed and caused implementation of requirements for the promulgation of acquisition system protection plans as a part of the procurement process. In many cases these plans are subject to review during the Defense Acquisition Board (DAB) process. The ASPWG effectively has struck down barriers that divided the security and procurement communities too long. The ASPWG and DISC are in a position to work as a team to assist in identification of broad areas of information that require protection.

A proposed reissuance of DoD Directive 5200.1 reestablishes the DISC at a high level. This new body is to be chaired by the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) (DASD(CI&SCM)) and be called the Security Classification and Safeguards Committee (SCSC). It provides a response to that part of Implementation Objective No. 1 that calls for establishment of a senior review panel to provide overall policy guidance. As noted, the new SCSC will be chaired by the DASD(CI&SCM). Membership will be comprised of the senior security classification and safeguards officials of DoD Components.

A pending revision of DoD 5200.1-R provides a response to another part of Implementation Objective No. 1, that is, it will provide an integrated policy approach for the identification and protection of both classified and unclassified sensitive information. It will integrate into one issuance DoD policy for the identification and protection of classified information as well as information that is For Official Use Only, UCNI, sensitive in the context of the Computer Security Act, distribution limited, Limited Official Use, and export controlled.

Further integration of processes can be achieved through adoption of new security policy that would encourage or require development and promulgation of security classification guidance for organizations such as a DoD Component or an office. Such mission-oriented guidance could cover the full range of sensitivities that the Component or office confronts on a routine basis. For example, in a personnel office, it could identify those Privacy Act details as well as the classification of the identities of clandestine intelligence operatives that appear in the personnel records collection. This is essential to a total quality approach to the protection of DoD information resources.

The disparity between policy and practice in the fields of original and derivative security classification must be addressed at all levels to assure available security resources are expended only when required to safeguard properly classified information. The Department of Defense Security Institute has launched the "Classification Management" course. The four yearly iterations of this course should improve DoD performance in this critical area. The criticality comes from the fact that the decision to classify drives application of other security resources. The importance of this new course offering should be briefed to the DISC. In turn, the DISC members should be tasked to help identify those DoD Component personnel who might benefit most from attendance at the "Classification Management" course.

- **Definition of Approach**. To apply internal CI&SCM resources to solving the problems identified, the DASD(CI&SCM) will chair a series DISC (or SCSC) meetings, with ASPWG participation, to address this report. The DISC will, in the interim, act as the "senior review panel" and consider its relationship to a blue-ribbon panel of great Americans to be formed in the next stages of this effort. Too, the DISC will consider whether, in the long haul, it should be the "senior review panel" contemplated in Implementation Objective No. 1. The DISC also will consider the advantages and disadvantages of a panel composed of very senior DoD personnel versus a panel of "great Americans" who would not necessarily be or have been affiliated with the Department of Defense. Inclusion of these alternatives at this point in the development of a complete response to Implementation Objective No. 1 is to assure barriers to options are removed and the widest range of views is considered.

The DISC, and any invited additional DoD agency or working group representatives, will make preparations for future work of the blue-ribbon panel by collecting and analyzing extant information protection studies and developing a synthesis of those for higher-level consideration. Working from that point, an existing study may be adopted or a new one developed by the DISC.

Additionally, the DISC will continue to advise and assist the Information Systems Security Directorate, ODASD(CI&SCM) in the preparation of a new issue of DoD 5200.1-R that will provide a unified policy document for protection of both classified and sensitive but unclassified information within the Department of Defense.

Though a DoD initiative, it is envisioned that the blue-ribbon panel report ultimately may need to be sent to the President for consideration and further action at the national level. That action could take the form of an Executive order implementing the FOIA and other statutes which would support a unified information protection structure at the national level. Also, that action

could take the form of proposed legislation to rationalize existing statutes and provide a statutory basis for the present security classification system. Other possibilities may be developed by the blue-ribbon panel for presentation to the President.

- **Reports**. The DISC/ASPWG will report progress to the ASD(C3I).

REVIEWED AND APPROVED:

Charles A. Hawkins, Jr.
Acting Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)

DATE:

APPENDIX A

ASD(C3I) Memorandum of June 4, 1992

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON D C 20301 3040

June 4, 1992

COMMAND CONTROL
COMMUNICATIONS
AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Defense Counterintelligence and Security Countermeasures Strategic Plan

Aggressive and focused counterintelligence and security countermeasures efforts within the Department of Defense are required to safeguard the people, material and functions that are contributing to the security of our nation. To strengthen these efforts, I have approved the attached Defense Counterintelligence and Security Countermeasures Strategic Plan.

Request that the Chairman of the Joint Chiefs of Staff communicate the contents of the subject plan to the Commanders of the Unified and Specified Combatant Commands.

Duane P. Andrews

DEFENSE COUNTERINTELLIGENCE AND SECURITY COUNTERMEASURES

STRATEGIC PLAN

INTRODUCTION

Taking into account the end of the Cold War and adjustments in the new world environment, this plan sets forth a course of action to rationalize and strengthen counterintelligence and security countermeasures (CI & SCM) as requested by the Secretary of Defense in the "Plan for Restructuring Defense Intelligence," approved on March 15, 1991. As directed by the Secretary, all CI & SCM activities, except for those involving Special Access Programs (SAPs) and international and NATO security matters, were transferred from the Under Secretary of Defense for Policy (USD(P)) to the Assistant Secretary of Defense for Command, Control , Communications and Intelligence (ASD(C3I)), thus establishing a closer relationship with Department of Defense (DoD) intelligence and information activities. To further strengthen the Department's information protection activities, the ASD(C3I) combined information security with counterintelligence and security countermeasures and created a Deputy Assistant Secretary position to manage the programs. This strategic plan complements the recent realignments of personnel and responsibilities within the Office of the Secretary of Defense.

Counterintelligence and security countermeasures protect the national security by safeguarding people, facilities, technology, information systems , and materials against terrorism and crime, espionage, or sabotage, conducted for or on behalf of a foreign power, organizations, or persons. CI & SCM include under their cognizance, as a minimum: counterintelligence investigations, operations, production, and collection; material classification and safeguards; personnel, physical, industrial, and systems security; and those measures employed to prevent the disclosure, loss, misuse or destruction of national security information, materials, or the systems and networks used to collect, process, analyze, store, or communicate that information. Effective CI & SCM counter, deter, exploit, and elude efforts to diminish our Nation's defense capabilities.

THE VISION

The CI & SCM community needs a flexible structure within which it can create and provide integrated CI & SCM services for both policymakers and warfighters. This structure will expand the strategies for CI collection, operations, investigations and production through a master plan that delineates CI & SCM interoperability in the dynamically changing world in the next ten years. This structure will also serve designers, implementers, and users of DoD systems and networks, and support the understanding and development of strategies, tactics, and contingency plans likely to be employed in crisis situations or on future battlefields. It will enhance the protection of weapon systems critical to battlefield success, as well as the development of follow-on systems throughout the entire research and development cycle. Essentially, the structure will:

- coherently address the problems of intelligence threat identification, characterization, and neutralization;
- conduct risk and vulnerability assessments;
- develop standards and policies on which to base the validation of CI & SCM requirements;
- cope with complex legal and legislative issues;
- take advantage of evolving technologies, both at costs and within time periods that are both rational and realistic given expected Defense budget levels in the next ten years;
- bring CI into the arena of joint operations as a key contributor;
- respond to requirements targeting nontraditional, non-standard threats (e.g., terrorism, narcotics) with a minimal impact on daily operations;
- develop viable strategies for CI support to HUMINT and for Offensive CI Operations;
- develop strategies to ensure that CI & SCM is an integral part of the acquisition process; and,
- develop strategies to maximize CI & SCM support to operations of the Military Departments.

CURRENT SITUATION, TRENDS, AND ANALYSIS

The demise of the Soviet Government and its clients in the central and eastern European states has radically altered the nature of the foreign intelligence threat faced by the US Government and the Department of Defense (DoD) worldwide. The implications for the US counterintelligence (CI) and security countermeasures (SCM) community are enormous. Recent developments have highlighted economic espionage, diversion of military and defense-related technology, US positions and intentions involving regional conflicts and threats posed to US military assets involved in counterdrug, counterinsurgency, and internal defense and development operations as the current high priority targets for foreign intelligence, terrorist, and criminal organizations. The widespread availability of state-of-the-art communications, cryptographic, and other electronic equipment, coupled with the increasing vulnerability of information systems to high-technology threats, such as computer viruses, will pose additional national security concerns. In response, a redirection of priorities and the development of new responses within the military counterintelligence and security countermeasures community are required.

The demise of the Soviet threat has also caused deep cuts in the US Defense Budget and further cuts must be anticipated. This means there will be reduced CI & SCM resources to meet future foreign intelligence, terrorist, and criminal threats to the US military. Therefore, the efficient, coordinated and frugal use of US Defense CI & SCM resources becomes of paramount necessity.

In the past, US counterintelligence efforts and security countermeasures were designed primarily to deal with the high-level of expertise and technical sophistication possessed by the Soviet intelligence services and their clients. The current and future world environment will present a diverse array of threats with widely varying levels of sophistication and technical expertise. This diverse threat environment, combined with diminished resources, will demand greater flexibility in terms of the application of CI & SCM procedures in neutralizing the varying foreign intelligence, terrorist, and criminal threats posed to US defense assets.

The advances in computer technology and telecommunications incorporated into US defense systems and equipment have also created a vastly different category of vulnerabilities than those seen only 5 years ago. Thousands of pages of classified material can be carried in a coat pocket. Millions of dollars worth of software can be destroyed with a phone call. In the past, information systems security considerations have not always been incorporated into automated information systems from their inception. This has resulted in costly attempts to integrate information security systems into DoD automated systems after the fact, many of which have proven constraining and ineffective. The DoD CI & SCM community must devise methods to eliminate these costly and ineffective attempts to retrofit and ensure that information security systems are designed into DoD automated systems from their inception.

An additional factor that will impact adversely on DoD CI & SCM effectiveness is the perception that the threat has "gone away." A commander or policymaker/decisionmaker will not expend resources or constrain operations unless he/she is fully and effectively informed of the threat that foreign intelligence, terrorist, and criminal organizations really present. In the future, the DoD CI & SCM community will be required more than ever to define the threat and demonstrate the effectiveness of proposed methods to defeat and elude it.

The "volunteer" spy, a trusted US citizen who betrays his/her own country for money, will continue to be a threat. The major buyers may change from the Soviets to narcotics traffickers, economic competitors, and, in some cases, even "friends," as in the Pollard case, but the threat will remain. The changing threat environment may witness a wider diversity in motivations for espionage.

Major goals, guiding principles, and objectives to support a renewed CI & SCM effort are listed on the following pages.

LONG-TERM GOALS

The goals of CI & SCM are to:

- Enhance at all echelons the understanding of threats facing the US National interests and programs for the next ten years.

- Improve our management of CI & SCM across the spectrum of disciplines as an aid to total integration of protective measures.

- Protect the US technological edge within the world economic structure and the US readiness posture vis-a-vis its role in the world.

- Establish a better quality and cost-effective CI & SCM customer/user support system which is executable at all echelons.

- Foster innovation and creative research and development designed to ensure and protect US security well into the 21st Century.

GUIDING PRINCIPLES

In achieving our goals, the following guiding principles apply:

- Centralize and streamline the performance of CI & SCM. Take full advantage of economies of scale where centralization of functions can satisfy requirements for provision of CI & SCM services. Apply technological solutions where cost-effective in order to reduce dependence on expensive personnel and facilities.

- Maintain close and continuing coordination with agencies and organizations pursuing disciplines related to CI & SCM. Obtain maximum value from CI & SCM-related information and experience by sharing with U.S. law enforcement and intelligence agencies and organizations, as well as those of host countries where appropriate, and obtaining access to their information and experience in return.

- Lower costs across the board. Seek innovative ways to reduce fixed costs over the long term. Use commercial off-the-shelf (COTS) or non-developmental item (NDI) technology where feasible. Recognize that success and endurability of future systems will be predicated, in large part, on effective cost control.

- Maintain the effectiveness of CI & SCM personnel and enhance their skills consistent with changes in the CI & SCM mission. Maintain suitable career paths for civilian and military cadres, train and prepare managers for higher responsibility, and provide in the work force the mix of skills and experience necessary to transition from today's environment to that of the future.

- Achieve a total quality discipline in CI & SCM. Provide an environment in which the absence of inefficiencies is the key to lower costs and higher satisfaction at the user end of CI & SCM services. Maintain a close relationship with those for whom we provide CI & SCM services, constantly analyzing the benefits that CI & SCM provide to their missions.

CI AND SCM STRATEGY

1. IMPLEMENTATION OBJECTIVE: Prioritize which information needs protection, the threat through loss (and to whom), and the protection necessary.

THE STATUS: The development of guidance for determining the classification of information or designating unclassified information as sensitive is fragmented across numerous components and organizations. As a result, there is no standard process that would consider the value of the information to be protected to our policymakers and warfighters, or for determining the priority of the application of protective resources to classified or unclassified sensitive information. Moreover, DoD Components and organizations are attempting to define the threat to this information based on their own necessarily limited version of the national security environment. Further complicating this situation, information that is crucial to decision-making and warfighting (but that is not necessarily classified) increasingly resides on and is shared between automated information systems without requisite security considerations having been included in the design of the data networking process. Overall, this fragmentation of policy development has resulted in inadequate cost benefits analysis, uneven security levels, significant redundancy, cost escalation, and managerial inefficiencies. Fiscal responsibility dictates that we must carefully define what must be protected and concentrate our finite resources upon safeguarding our most important assets and information. This requires a fundamentally new way of thinking about the "security envelope" to be applied to our information and information systems in the post-Cold War period.

IMPLEMENTATION ACTION: By July 30, 1992, the ASD(C3I) will review the processes used for determining classification of information and designation of sensitive information, and develop an integrated approach -- to include establishment of a senior review panel to provide cohesive and overall policy guidance-- that identifies, defines, and prioritizes the categories of information that require protection so that CI & SCM organizations can direct their shrinking resources to the most critical areas.

2. IMPLEMENTATION OBJECTIVE: Streamline and improve management oversight, operational review, mission execution, and cross-discipline analysis of CI & SCM programs.

THE STATUS: The reorganization of CI & SCM within OSD into a single functional area is designed to improve coordination and management across the disciplines. An initial, critical step is to define clearly the programs under DASD (CI & SCM) cognizance. Budget development, review, execution, and oversight of DoD security programs previously have not been centralized, integrated, or comprehensive; rather, SCM resources have been embedded in other major force programs, making accounting and oversight extremely difficult. Moreover, the CI program, while planned and budgeted for by DoD as part of the National Foreign Intelligence Program (NFIP), has not had a mechanism to ensure budget execution review or overall strategic analysis. Information Security Systems (INFOSYSEC) program efforts are distributed widely across DoD agencies and organizations, and the lack of collective review and overall management virtually ensures that some programs overlap and significant gaps in capability exist.

Congress has directed that a report be submitted to the two intelligence committees by July 1, 1992, which discusses various alternatives in submitting an integrated CI & SCM program budget. We have contracted with the Institute for Defense Analyses (IDA) for support of these tasks; this includes identifying all programs and budgets throughout DoD that are associated with CI & SCM.

Congress also directed the transfer of 20 billets from the Military Departments to the Intelligence Program Support Group (IPSG) this fiscal year. These new resources will help improve the management of CI&SCM by performing program evaluation, cross program analysis, budget displays, and budget execution reviews.

IMPLEMENTATION ACTION: The ASD(C3I), in coordination with the DoD Components, will:

- By July 1, 1992, define those programs to be included in CI & SCM, and determine the best method to manage the CI & SCM budgets.

- By October 1, 1992, develop a plan for providing guidance to DoD agencies and organizations with regard to program overlap and gaps in existing information systems security programs.

- By December 15, 1992, clearly define CI & SCM support, and the roles of various organizations, to the DoD Acquisition process.

- By December 15, 1992, ensure the IPSG is adequately staffed to establish stronger program review of CI & SCM funding and to develop standards for consideration of cross program tradeoffs.

3. IMPLEMENTATION OBJECTIVE: Refocus CI efforts to protect DoD information (Objective 1) and improve CI responsiveness to the needs of the Military Services, OSD, the unified and specified commands, and the Chairman of the Joint Chiefs of Staff.

THE STATUS: For the past 40 years, the DoD CI community has focused a majority of its energies at defending the U.S. military against the intelligence threat posed by the Warsaw Pact and the People's Repubic of China. This orientation was in consonance with our strategic priorities; however, it left us with a dearth of knowledge and capabilities regarding nontraditional adversaries. Over the past decade and encouraged by the political changes in Eastern Europe, our realization of the threat posed by nuclear proliferation and technology transfer to unstable regional powers, e.g. Iraq, has been sharpened. Concomitantly, the threat posed to our HUMINT programs and expanding data automation networks by foreign intelligence services has been highlighted by disclosures from Eastern Europe and elsewhere.

Our CI focus must react appropriately to evolving National Security Strategies. Recent efforts by the US CI community, in which DoD CI is a major player, to better identify and understand the intelligence threat posed by nontraditional adversaries have been a necessary first step. Additionally, the inclusion of CI Support Officers (CISOs) on the staffs of the unified and specified combatant commands during the last two years is facilitating improved CI support. The establishment of a CI staff support office responsive to the DIA J-2 provides the impetus for the development of comprehensive joint CI doctrine, strategies, architectures, procedures, and systems to achieve effective interoperable CI support to the Chairman of the Joint Chiefs of Staff and unified and specified commands.

IMPLEMENTATION ACTION: By August 31,1992, the ASD(C3I) will set forth a CI strategy identifying assumptions, objectives and priorities for the remainder of the decade, in concert with the SECDEF Defense Planning Guidance and unified and specified command needs. In turn, this strategy would be implemented by the Defense counterintelligence agencies. The strategy would serve to guide all DoD CI agencies in refining the focus of their respective activities. The strategy would also eliminate the "Counter Warsaw Pact" orientation of past decades and bring DoD CI into a more global venue. It should reflect the heightened priority towards stopping proliferation, supporting HUMINT and military contingencies, and neutralizing the pertinent aspects of foreign intelligence attempts at penetrating DoD information systems and networks. Finally, the strategy should encourage closer integration of all source threat data to be shared among the CI agencies and appropriately interfaced with Defense security programs.

4. IMPLEMENTATION OBJECTIVE: Establish mechanisms to ensure that appropriate information security policies are implemented as part of all corporate information management (CIM) architectures, networks and systems.

THE STATUS: The principles of CIM are applicable to information systems architectures, networks, and systems under consideration for, or being developed by, the Department of Defense. Information security policies, requirements, procedures and protocols must be incorporated from the inception of our architectures, networks and systems. The Defense Information Systems Security Program (DISSP) under ASD(C3I) oversight, will manage, coordinate and direct support to DoD programs, develop standards and protocols in accordance with CI & SCM policy for information systems security, and expedite the implementation of multilevel secure (MLS) command, control, and communications systems for DoD.

IMPLEMENTATION ACTION: Effective immediately, ASD (C3I)/DASD (CI & SCM) will ensure INFOSEC participation in the development and evolution of DoD's CIM information systems architecture, and will oversee the DISSP's management of implementation of information security within DoD programs and the insertion of MLS technology.

5. IMPLEMENTATION OBJECTIVE: Establish effective and efficient processes and common standards for determining security clearance eligibility.

THE STATUS: National Security Directive 63 created the Single Scope Background Investigation to set common investigative standards for use by all Federal Agencies in determining the basis for clearance decisions for access to Top Secret and Sensitive Compartmented Information (SCI). More effort is underway, as a product of the National Industrial Security Program, to establish a single background investigative request form and common adjudication standards to ensure reciprocity among agencies.

Defense Management Review Decision (DMRD) 986 directed the Defense Personnel Security Research Center (PERSEREC) to conduct a study on consolidation of the adjudication process. PERSEREC has identified alternatives which are currently under review with ASD(C3I) and the Defense Components. After full coordination, recommendations will be forwarded to Deputy Secretary of Defense for final determination.

IMPLEMENTATION ACTION: The ASD (C3I), in coordination with the DoD Components, will:

- Within 90 days of approval of DMRD 986 by the Deputy Secretary of Defense, formulate an action plan to implement the consolidation alternative selected. The principles of corporate information management will be an integral part of the plan.

- By December 31, 1992, in further coordination with members of the National Industrial Security Program, establish.common and reciprocal standards for adjudication guidelines and appeals procedures.

6. IMPLEMENTATION OBJECTIVE: Develop more viable, attractive career paths, improved professional standards, and enhanced cross-training for CI & SCM personnel.

THE STATUS: DoD Components view counterintelligence and security countermeasures differently, and thus, are organized disparately. For example, the Navy and Air Force view CI as predominately an element of law enforcement, and therefore have combined CI and criminal investigative personnel into one command (e.g., the FBI model). On the other hand, the Army has viewed CI as an element of intelligence and has integrated it into intelligence units, while assigning the criminal investigative function to a separate major command (e.g,. the CIA model). Information Systems Security and Operations Security officials are scattered throughout, but most often are located in the information management or operations organizations.

Due to the difference in organizational structures, CI & SCM personnel tend to become focused, or specialized, in a particular area of expertise. While some specialization is desirable, a well-defined career program is required for professionals who advance to mid-and upper-level management ranks. This would maximize the DoD's ability to attract and retain the best qualified personnel, and therefore have the quality, consistency, and preparedness necessary to meet CI & SCM challenges.

IMPLEMENTATION ACTION: The ASD (C3I), in coordination with the ASD (FM&P) and other DoD Components, will :

- By June 15, 1993, complete a review and establish policies to develop a distinct career path for CI & SCM professionals that includes broadening opportunities and cross training. Minimum training standards for all levels of the military and civilian CI & SCM workforce will also be established; concurrently, improved consistency in career paths between DoD components will be addressed.

7. IMPLEMENTATION OBJECTIVE: Improve security and counterintelligence awareness among DoD functional managers and supervisors.

THE STATUS: Currently, there is no mandatory security countermeasures component included in general managerial and supervisory training and education programs. Therefore, DoD managers and supervisors often do not understand that sound security practices are important facets of their responsibilities. For those who do receive security education and training, the programs and materials are often inadequate, or out-of-date, and thus, are not well-received. In many cases, DoD managers and supervisors are not trained to detect, recognize, report, react to, or anticipate CI & SCM-related events. As a result, time is lost and risk of disclosure, misuse, compromise, or destruction of information systems, and harm to personnel and facilities, is increased.

IMPLEMENTATION ACTION: By August 15, 1992, the ASD (C3I) will:

- Define an improved, high quality security awareness program for use by all DoD and contractor employees. The DoD Security Institute will develop, in coordination with all DoD CI & SCM elements, as well as the intelligence, law enforcement, and private industry communities, a series of advisories and instructional modules that outline the range of vulnerabilities and the capabilities of these organizations to deal with threats. The modules will acquaint managers and supervisors with reporting requirements, protocols and procedures to use when they suspect that they are confronted with CI & SCM problems.

- Promote, through the Advisory Group/Security Countermeasures (AG/SCM) forum, the concept of common instructional standards for CI & SCM throughout the community as outlined in National Security Review 18.

8. IMPLEMENTATION OBJECTIVE: Improve research and development programs in all CI & SCM disciplines.

THE STATUS: CI & SCM research and development must be structured to improve our understanding of the future threat, to better account for evolving systems and networks, and to sponsor innovative solutions to security vulnerabilities. Pockets of research (albeit rudimentary) do exist; for example, a number of studies have been conducted recently into the features of American spy cases which have provided useful new approaches to prevent and detect espionage. Similarly, some research and development into the use of the polygraph and follow-on systems as tools for screening and investigation continues. In the information security arena, some studies which have exploited technology offer new options for establishing trusted systems. In no instance, however, does DoD have a central means to acquire, analyze, correlate, exploit, integrate, abstract, and disseminate CI & SCM-related research.

IMPLEMENTATION ACTION: By September 1, 1992, the ASD (C3I), in coordination with Director, Defense Research and Engineering, will:

- Define a program of research and development across the CI & SCM disciplines, including projects, programs, and activities within and among Government Agencies, academia, and private industry; facilitate the exchange of information concerning existing and evolving capabilities and

technologies; and sponsor active research at both the basic and applied levels. At a minimum, this program will sponsor a speedy multi-level secure (MLS) solution to DoD information management, examine follow-on systems or alternatives to the polygraph, and explore cost-effective technical solutions for physical security.

- Establish and maintain a CI & SCM research information analysis focal point to coordinate research, and designate appropriate DoD Agencies, organizations, institutes, and research facilities as Defense CI & SCM Research Centers responsible for conducting or monitoring of research in a given area, and for advising the Components on research results and efficiency.

CONCLUSION

The strategy of CI & SCM in the coming years is designed to provide more effective management and customer support -- to senior policy makers, warfighters, industry officials, arms control inspectors, acquisition experts, law enforcers, and designers, implementers, and users of DoD information systems. Our measure of success for CI & SCM programs will be judged by the quality, timeliness, affordability, comprehensiveness, and rationality of the protection packages tailored to these customers, and the degree to which they can use the programs for near-term investment decisions and long-range mission accomplishments.

CI & SCM programs must be implemented within the context of a dynamic, rapidly changing international and domestic environment, and where technologies continue to multiply and proliferate at a high rate. Programs must be adaptable to change, and their success will require a commitment to acquire new skills and technologies, to seek out other points of view, and to find and engage new opportunities. This will require strong discipline, especially in the area of cost control, in order to meet mission requirements while protecting adequately US personnel and the Nation's secrets, sensitive information, and vital infrastructure.

As part of the ongoing CI & SCM improvement process, this plan will be reviewed annually and changes made as necessary.

APPENDIX B

Selected Statutes

A. DISCLOSURE AND PROTECTION OF INFORMATION

SECTION 552 OF TITLE 5, UNITED STATES CODE (THE "FREEDOM OF INFORMATION ACT")

§ 552. Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public—

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying—

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; and

(C) administrative staff manuals and instructions to staff that affect a member of the public;

unless the materials are promptly published and copies offered for sale. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction. However, in each case the justification for the deletion shall be explained fully in writing. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of such index on request at a cost not to exceed the direct cost of duplication. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if—

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that—

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is

scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section—

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii) (II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed $250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo: *Provided*, That the court's review of the matter shall be limited to the record before the agency.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action.

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service

upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.

(E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acting arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall—

(i) determine within ten days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

(B) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working

days. As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular request—

(i) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(ii) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

(iii) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject-matter interest therein.

(C) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(d)

(b) This section does not apply to matters that are—

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be ex-

pected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and—

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to inerfere with enforcement proceedings,

the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requiements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically

stated in this section. This section does not authority to withhold information from Congress.

(e) On or before March 1 of each calendar year, each agency shall submit a report covering the preceding calendar year to the Speaker of the House of Representatives and President of the Senate for referral to the appropriate committees of the Congress. The report shall include—

(1) the number of determinations made by such agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(2) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information;

(3) the names and titles or positions of each person responsible for the denial of records requested under this section, and the number of instances of participation for each;

(4) the results of each proceeding conducted pursuant to subsection (a)(4)(F), including a report of the disciplinary action taken against the officer or employee who was primarily responsible for improperly withholding records or an explanation of why disciplinary action was not taken;

(5) a copy of every rule made by such agency regarding this section;

(6) a copy of the fee schedule and the total amount of fees collected by the agency for making records available under this section; and

(7) such other information as indicates efforts to administer fully this section.

The Attorney General shall submit an annual report on or before March 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subsections (a)(4)(E), (F) and (G). Such reports shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

(f) For purposes of this section, the term "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

SECTION 552a OF TITLE 5, UNITED STATES CODE (THE "PRIVACY ACT")

552a. Records maintained on individuals

(a) DEFINITIONS.—For purposes of this section—

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

the Government data necessary to incorporate change
design or technology.

(8) Before ordering any spare part, the contracting of
should review the acquisition history of that part.

AUTHORITY TO WITHHOLD FROM PUBLIC DISCLOSURE CERTAIN TECHNICAL DATA

SEC. 1217. (a) Chapter 4 of title 10, United States Code, is ame
by adding at the end thereof the following new section:

10 USC 140c.

**"§ 140c. Secretary of Defense: authority to withhold from p
disclosure certain technical data**

"(a) Notwithstanding any other provision of law, the Secreta
Defense may withhold from public disclosure any technical
with military or space application in the possession of, or unde
control of, the Department of Defense, if such data may n
exported lawfully outside the United States without an appr
authorization, or license under the Export Administration A
1979 (50 U.S.C. App. 2401-2420) or the Arms Export Control A
U.S.C. 2751 et seq.). However, technical data may not be with
under this section if regulations promulgated under either such
authorize the export of such data pursuant to a general,
stricted license or exemption in such regulations.

Regulations.

"(b)(1) Within 90 days after enactment of this section, the S
tary of Defense shall propose regulations to implement this sec
Such regulations shall be published in the Federal Register
period of no less than 30 days for public comment before prom
tion. Such regulations shall address, where appropriate, releas
technical data to allies of the United States and to qualified U
States contractors, including United States contractors that
small business concerns, for use in performing United States
ernment contracts.

Publication in Federal Register

"Technical data with military or space application."

"(2) In this section, 'technical data with military or space ap
tion' means any blueprints, drawings, plans, instructions, com
software and documentation, or other technical information
can be used, or be adapted for use, to design, engineer, proc
manufacture, operate, repair, overhaul, or reproduce any mil
or space equipment or technology concerning such equipme

(b) The table of sections at the beginning of chapter 4 of such
is amended by adding at the end thereof the following new

"140c. Secretary of Defense: authority to withhold from public disclosure c
technical data."

USE OF POLYGRAPHS BY THE DEPARTMENT OF DEFENSE

SEC. 1218. (a) The Secretary of Defense may not, before Apr
1984, use, enforce, issue, implement, or otherwise rely on any
regulation, directive, policy, decision, or order that would permi
use of polygraph examinations in the case of civilian employe
the Department of Defense or members of the Armed Forces i
manner or to any extent greater than was permitted under
regulations, directives, policies, decisions, or orders of the De
ment of Defense in effect on August 5, 1982.

(b) The restrictions prescribed in subsection (a) with respect t
use of polygraph examinations in the Department of Defense

B. NATIONAL SECURITY AGENCY

NATIONAL SECURITY AGENCY ACT OF 1959

PUBLIC LAW 86-36—MAY 29, 1959

(50 U.S.C. 402 note)

AN ACT To provide certain administrative authorities for the National Securit Agency, and for other purposes.

Be it enacted by the Senate and House of Representatives of t United States of America in Congress assembled, That this Act m be cited as the "National Security Agency Act of 1959".

SEC. 2. The Secretary of Defense (or his designee for the purpo is authorized to establish such positions, and to appoint there without regard to the civil service laws, such officers and emplo ees, in the National Security Agency, as may be necessary to car out the functions of such agency. The rates of basic compensati for such positions shall be fixed by the Secretary of Defense (or h designee for the purpose) in relation to the rates of basic compens tion contained in the General Schedule of the Classification Act 1949, as amended,[1] for positions subject to such Act which ha corresponding levels of duties and responsibilities. Except as pr vided in subsections (f) and (g) of section 303 of the Federal Exec tive Salary Act of 1964,[2] no officer or employee of the National S curity Agency shall be paid basic compensation at a rate in exce of the highest rate of basic compensation contained in such Gene al Schedule. Not more than seventy such officers and employe shall be paid basic compensation at rates equal to rates of bas compensation contained in grades 16, 17, and 18 of such Gener Schedule.

SEC. 3. [Section 3 consisted of amendments to section 1581(a) title 10, United States Code.]

SEC. 4. The Secretary of Defense (or his designee for the purpos is authorized to—

(1) establish in the National Security Agency (A) profession engineering positions primarily concerned with research an development and (B) professional positions in the physical an natural sciences, medicine, and cryptology; and

(2) fix the respective rates of pay of such positions at rate equal to rates of basic pay contained in grades 16, 17, and 18

[1] The Classification Act of 1949 was repealed by the law enacting title 5, United States Co (Public Law 89-554, Sept. 6, 1966, 80 Stat. 378). The General Schedule for civilian employees now set out at section 5332 of title 5.

[2] The Federal Executive Salary Act of 1964 was repealed by the law enacting title 5, Unite States Code (Public Law 89-554, Sept. 6, 1966, 80 Stat. 378). See sections 5316 and 5317 of title United States Code.

the General Schedule set forth in section 5332 of title 5, United States Code.

Officers and employes appointed to positions established under this section shall be in addition to the number of officers and employees appointed to positions under section 2 of this Act who may be paid at rates equal to rates of basic pay contained in grades 16, 17, and 18 of the General Schedule.

SEC. 5. Officers and employees of the National Security Agency who are citizens or nationals of the United States may be granted additional compensation, in accordance with regulations which shall be prescribed by the Secretary of Defense, not in excess of additional compensation authorized by section 207 of the Independent Offices Appropriation Act, 1949, as amended (5 U.S.C. 118h),[3] for employees whose rates of basic compensation are fixed by statute.

SEC. 6. (a) Except as provided in subsection (b) of this section, nothing in this Act or any other law (including, but not limited to, the first section and section 2 of the Act of August 28, 1935 (5 U.S.C. 654)[4]) shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

(b) The reporting requirements of section 1512 of title 10, United States Code, shall apply to positions established in the National Security Agency in the manner provided by section 4 of this Act.

SEC. 7. [Section 7 was repealed by section 8(a) of Public Law 89-554 (September 6, 1966, 80 Stat. 660).]

SEC. 8. The foregoing provisions of this Act shall take effect on the first day of the first pay period which begins later than the thirtieth day following the date of enactment of this Act.

SEC. 9. (a) Notwithstanding section 322 of the Act of June 30, 1932 (40 U.S.C. 278a), section 5536 of title 5, United States Code, and section 2675 of title 10, United States Code, the Director of the National Security Agency, on behalf of the Secretary of Defense, may lease real property outside the United States, for periods not exceeding ten years, for the use of the National Security Agency for special cryptologic activities and for housing for personnel assigned to such activities.

(b) The Director of the National Security Agency, on behalf of the Secretary of Defense, may provide to certain civilian and military personnel of the Department of Defense who are assigned to special cryptologic activities outside the United States and who are designated by the Secretary of Defense for the purposes of this subsection—

(1) allowances and benefits—

(A) comparable to those provided by the Secretary of State to members of the Foreign Service under chapter 9 of title I of the Foreign Service Act of 1980 (22 U.S.C. 4081 et seq.) or any other provision of law; and

[3] The Independent Offices Appropriation Act, 1949, was repealed by the law enacting title 5, United States Code (Public Law 89-554, Sept 6, 1966, 80 Stat. 377). Section 207 of that Act was codified as section 5941 of title 5, United States Code.

[4] Repealed by section 101 of Public Law 86-626 (July 12, 1960, 74 Stat. 427).

(B) in the case of selected personnel serving in circumstances similar to those in which personnel of the Central Intelligence Agency serve, comparable to those provided by the Director of Central Intelligence to personnel of the Central Intelligence Agency (including special retirement accrual in the same manner provided in section 303 of the Central Intelligence Agency Retirement Act of 1964 for Certain Employees (50 U.S.C. 403 note)); and

(2) housing (including heat, light, and household equipment) without cost to such personnel, if the Director of the National Security Agency, on behalf of the Secretary of Defense determines that it would be in the public interest to provide such housing.

(c) The authority of the Director of the National Security Agency, on behalf of the Secretary of Defense, to make payments under subsections (a) and (b), and under contracts for leases entered into under subsection (a), is effective for any fiscal year only to the extent that appropriated funds are available for such purpose.

(d) Members of the Armed Forces may not receive benefits under both subsection (b)(1) and title 37, United States Code, for the same purpose. The Secretary of Defense shall prescribe such regulations as may be necessary to carry out this subsection.

(e) Regulations issued pursuant to subsection (b)(1) shall be submitted to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate before such regulations take effect.

SEC. 10. (a) The Director of the National Security Agency shall arrange for, and shall prescribe regulations concerning, language and language-related training programs for military and civilian cryptologic personnel. In establishing programs under this section for language and language-related training, the Director—

(1) may provide for the training and instruction to be furnished, including functional and geographic area specializations;

(2) may arrange for training and instruction through other Government agencies and, in any case in which appropriate training or instruction is unavailable through Government facilities, through nongovernmental facilities that furnish training and instruction useful in the fields of language and foreign affairs;

(3) may support programs that furnish necessary language and language-related skills, including, in any case in which appropriate programs are unavailable at Government facilities, support through contracts, grants, or cooperation with nongovernmental educational institutions; and

(4) may obtain by appointment or contract the services of individuals to serve as language instructors, linguists, or special language project personnel.

(b)(1) In order to maintain necessary capability in foreign language skills and related abilities needed by the National Security Agency, the Director, without regard to subchapter IV of chapter 56 of title 5, United States Code, may provide special monetary or

other incentives to encourage civilian cryptologic personnel of the Agency to acquire or retain proficiency in foreign languages or special related abilities needed by the Agency.

(2) In order to provide linguistic training and support for cryptologic personnel, the Director—

(A) may pay all or part of the tuition and other expenses related to the training of personnel who are assigned or detailed for language and language-related training, orientation, or instruction; and

(B) may pay benefits and allowances to civilian personnel in accordance with chapters 57 and 59 of title 5, United States Code, and to military personnel in accordance with chapter 7 of title 37, United States Code, and applicable provisions of title 10, United States Code, when such personnel are assigned to training at sites away from their designated duty station.

(c)(1) To the extent not inconsistent, in the opinion of the Secretary of Defense, with the operation of military cryptologic reserve units and in order to maintain necessary capability in foreign language skills and related abilities needed by the National Security Agency, the Director may establish a cryptologic linguist reserve. The cryptologic linguist reserve may consist of former or retired civilian or military cryptologic personnel of the National Security Agency and of other qualified individuals, as determined by the Director of the Agency. Each member of the cryptologic linguist reserve shall agree that, during any period of emergency (as determined by the Director), the member shall return to active civilian status with the National Security Agency and shall perform such linguistic or linguistic-related duties as the Director may assign.

(2) In order to attract individuals to become members of the cryptologic linguist reserve, the Director, without regard to subchapter IV of chapter 55 of title 5, United States Code, may provide special monetary incentives to individuals eligible to become members of the reserve who agree to become members of the cryptologic linguist reserve and to acquire or retain proficiency in foreign languages or special related abilities.

(3) In order to provide training and support for members of the cryptologic linguist reserve, the Director—

(A) may pay all or part of the tuition and other expenses related to the training of individuals in the cryptologic linguist reserve who are assigned or detailed for language and language-related training, orientation, or instruction; and

(B) may pay benefits and allowances in accordance with chapters 57 and 59 of title 5, United States Code, to individuals in the cryptologic linguist reserve who are assigned to training at sites away from their homes or regular places of business.

(d)(1) The Director, before providing training under this section to any individual, may obtain an agreement with that individual that—

(A) in the case of current employees, pertains to continuation of service of the employee, and repayment of the expenses of such training for failure to fulfill the agreement, consistent with the provisions of section 4108 of title 5, United States Code; and

(B) in the case of individuals accepted for membership in cryptologic linguist reserve, pertains to return to service wl requested, and repayment of the expenses of such training failure to fulfill the agreement, consistent with the provisi of section 4108 of title 5, United States Code.

(2) The Director, under regulations prescribed under this secti may waive, in whole or in part, a right of recovery under an agr ment made under this subsection if it is shown that the recov would be against equity and good conscience or against the pul interest.

(e)(1) Subject to paragraph (2), the Director may provide to fam members of military and civilian cryptologic personnel assigned representational duties outside the United States, in anticipation the assignment of such personnel outside the United States while outside the United States, appropriate orientation and la guage training that is directly related to the assignment abroad.

(2) Language training under paragraph (1) may not be provid to any individual through payment of the expenses of tuition other cost of instruction at a non-Government educational instit tion unless appropriate instruction is not available at a Gover ment facility.

(f) The Director may waive the applicability of any provision chapter 41 of title 5, United States Code, to any provision of th section if he finds that such waiver is important to the perforn ance of cryptologic functions.

(g) The authority of the Director to enter into contracts or t make grants under this section is effective for any fiscal year onl to the extent that appropriated funds are available for such pu pose.

(h) Regulations issued pursuant to this section shall be submitte to the Permanent Select Committee on Intelligence of the House o Representatives and the Select Committee on Intelligence of th Senate before such regulations take effect.

(i) The Director of the National Security Agency, on behalf of th Secretary of Defense, may, without regard to section 4109(a)(2)(B) o title 5, United States Code, pay travel, transportation, storage, an subsistence expenses under chapter 57 of such title to civilian an military personnel of the Department of Defense who are assigned to duty outside the United States for a period of one year or longe which involves cryptologic training, language training, or related disciplines.

SEC. 11. The Administrator of General Services, upon the application of the Director of the National Security Agency, may provide for the protection in accordance with section 3 of the Act of June 1, 1948 (40 U.S.C. 318b), of certain facilities (as designated by the Director of such Agency) which are under the administration and control of, or are used by, the National Security Agency in the same manner as if such facilities were property of the United States over which the United States has acquired exclusive or concurrent criminal jurisdiction.

SEC. 12. (a)(1) The Secretary of Defense (or his designee) may by regulation establish a personnel system for senior civilian cryptologic personnel in the National Security Agency to be known as the

Senior Cryptologic Executive Service. The regulations establishing the Senior Cryptologic Executive Service shall—

(A) meet the requirements set forth in section 3131 of title 5, United States Code, for the Senior Executive Service;

(B) provide that positions in the Senior Cryptologic Executive Service meet requirements that are consistent with the provisions of section 3132(a)(2) of such title;

(C) provide, without regard to section 2 rates of pay for the Senior Cryptologic Executive Service that are not in excess of the maximum rate or less than the minimum rate of basic pay established for the Senior Executive Service under section 5382 of such title, and that are adjusted at the same time and to the same extent as rates of basic pay for the Senior Executive Service are adjusted;

(D) provide a performance appraisal system for the Senior Cryptologic Executive Service that conforms to the provisions of subchapter II of chapter 43 of such title;

(E) provide for removal consistent with section 3592 of such title, and removal or suspension consistent with subsections (a), (b), and (c) of section 7543 of such title (except that any hearing or appeal to which a member of the Senior Cryptologic Executive Service is entitled shall be held or decided pursuant to procedures established by regulations of the Secretary of Defense or his designee);

(F) permit the payment of performance awards to members of the Senior Cryptologic Executive Service consistent with the provisions applicable to performance awards under section 5384 of such title; and

(G) provide that members of the Senior Cryptologic Executive Service may be granted sabbatical leaves consistent with the provisions of section 3396(c) of such title.

(2) Except as otherwise provided in subsection (a), the Secretary of Defense (or his designee) may—

(A) make applicable to the Senior Cryptologic Executive Service any of the provisions of title 5, United States Code, applicable to applicants for or members of the Senior Executive Service; and

(B) appoint, promote, and assign individuals to positions established within the Senior Cryptologic Executive Service without regard to the provisions of title 5, United States Code, governing appointments and other personnel actions in the competitive service.

(3) The President, based on the recommendations of the Secretary of Defense, may award ranks to members of the Senior Cryptologic Executive Service in a manner consistent with the provisions of section 4507 of title 5, United States Code.

(4) Notwithstanding any other provision of this section, the Director of the National Security Agency may detail or assign any member of the Senior Cryptologic Executive Service to serve in a position outside the National Security Agency in which the member's expertise and experience may be of benefit to the National Security Agency or another Government agency. Any such member shall not by reason of such detail or assignment lose any entitlement or status associated with membership in the Senior Cryptologic Executive Service.

(5) The Director of the National Security Agency shall each year submit to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, at the time the Budget is submitted by the President to the Congress for the next fiscal year, a report on executive personnel in the National Security Agency. The report shall include—

(A) the total number of positions added to or deleted from the Senior Cryptologic Executive Service during the preceding fiscal year;

(B) the number of executive personnel (including all members of the Senior Cryptologic Executive Service) being paid at each grade level and pay rate in effect at the end of the preceding fiscal year;

(C) the number, distribution, and amount of awards paid to members of the Senior Cryptologic Executive Service during the preceding fiscal year; and

(D) the number of individuals removed from the Senior Cryptologic Executive Service during the preceding fiscal year for less than fully successful performance.

(b) The Secretary of Defense (or his designee) may by regulation establish a merit pay system for such employees of the National Security Agency as the Secretary of Defense (or his designee) considers appropriate. The merit pay system shall be designed to carry out purposes consistent with those set forth in section 5401(a) of title 5, United States Code.

(c) Nothing in this section shall be construed to allow the aggregate amount payable to a member of the Senior Cryptologic Executive Service under this section during any fiscal year to exceed the annual rate payable for positions at level I of the Executive Schedule in effect at the end of such year.

SEC. 13. (a) The Director of the National Security Agency may make grants to private individuals and institutions for the conduct of cryptologic research. An application for a grant under this section may not be approved unless the Director determines that the award of the grant would be clearly consistent with the national security.

(b) The grant program established by subsection (a) shall be conducted in accordance with the Federal Grant and Cooperative Agreement Act of 1977 (41 U.S.C. 501 et seq.) to the extent that such Act is consistent with and in accordance with section 6 of this Act.

(c) The authority of the Director to make grants under this section is effective for any fiscal year only to the extent that appropriated funds are available for such purpose.

SEC. 14. Funds appropriated to an entity of the Federal Government other than an element of the Department of Defense that have been specifically appropriated for the purchase of cryptologic equipment, materials, or services with respect to which the National Security Agency has been designated as the central source of procurement for the Government shall remain available for a period of three fiscal years.

SEC. 15. (a) No person may, except with the written permission of the Director of the National Security Agency, knowingly use the words "National Security Agency", the initials "NSA", the seal of the National Security Agency, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the National Security Agency.

(b) Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

SEC. 16. (a) The purpose of this section is to establish an undergraduate training program, which may lead to the baccalaureate degree, to facilitate the recruitment of individuals, particularly minority high school students, with a demonstrated capability to develop skills critical to the mission of the National Security Agency, including mathematics, computer science, engineering, and foreign languages.

(b) The Secretary of Defense is authorized, in his discretion, to assign civilian employees of the National Security Agency as students at accredited professional, technical, and other institutions of higher learning for training at the undergraduate level in skills critical to effective performance of the mission of the Agency.

(c) The National Security Agency may pay, directly or by reimbursement to employees, expenses incident to assignments under subsection (b), in any fiscal year only to the extent that appropriated funds are available for such purpose.

(d)(1) To be eligible for assignment under subsection (b), an employee of the Agency must agree in writing—

(A) to continue in the service of the Agency for the period of the assignment and to complete the educational course of training for which the employee is assigned;

(B) to continue in the service of the Agency following completion of the assignment for a period of one-and-a-half years for each year of the assignment or part thereof;

(C) to reimburse the United States for the total cost of education (excluding the employee's pay and allowances) provided under this section to the employee if, prior to the employee's completing the educational course of training for which the employee is assigned, the assignment or the employee's employment with the Agency is terminated either by the Agency due to misconduct by the employee or by the employee voluntarily; and

(D) to reimburse the United States if, after completing the educational course of training for which the employee is assigned, the employee's employment with the Agency is terminated either by the Agency due to misconduct by the employee or by the employee voluntarily, prior to the employee's completion of the service obligation period described in subparagraph (B), in an amount that bears the same ratio to the total cost of the education (excluding the employee's pay and allowances) provided to the employee as the unserved portion of the service obligation period described in subparagraph (B) bears to the total period of the service obligation described in subparagraph (B).

(2) Subject to paragraph (3), the obligation to reimburse the United States under an agreement described in paragraph (1), including interest due on such obligation, is for all purposes a debt owing the United States.

(3)(A) A discharge in bankruptcy under title 11, United States Code, shall not release a person from an obligation to reimburse the United States required under an agreement described in paragraph (1) if the final decree of the discharge in bankruptcy is issued within five years after the last day of the combined period of service obligation described in subparagraphs (A) and (B) of paragraph (1).

(B) The Secretary of Defense may release a person, in whole or in part, from the obligation to reimburse the United States under an agreement described in paragraph (1) when, in his discretion, the Secretary determines that equity or the interests of the United States so require.

(C) The Secretary of Defense shall permit an employee assigned under this section who, prior to commencing a second academic year of such assignment, voluntarily terminates the assignment or the employee's employment with the Agency, to satisfy his obligation under an agreement described in paragraph (1) to reimburse the United States by reimbursement according to a schedule of monthly payments which results in completion of reimbursement by a date five years after the date of termination of the assignment or employment or earlier at the option of the employee.

(e)(1) When an employee is assigned under this section to an institution, the Agency shall disclose to the institution to which the employee is assigned that the Agency employs the employee and that the Agency funds the employee's education.

(2) Agency efforts to recruit individuals at educational institutions for participation in the undergraduate training program established by this section shall be made openly and according to the common practices of universities and employers recruiting at such institutions.

(f) Chapter 41 of title 5 and subsections (a) and (b) of section 3324 of title 31, United States Code, shall not apply with respect to this section.

(g) The Secretary of Defense may issue such regulations as may be necessary to implement this section.

(b) The authority conferred by this section may be delegated by the Secretary of Defense to any person in the Department of Defense or by the Secretary of a military department to any person within his department, with or without the authority to make successive redelegations.

(c) In any case in which funds are expended under the authority of subsections (a) and (b), the Secretary of Defense shall submit a report of such expenditures on a quarterly basis to the Committees on Armed Services and Appropriations of the Senate and the House of Representatives.

(Added Pub. L. 94-106, title VIII, § 804(a), Oct. 7, 1975, 89 Stat. 538, § 140; amended Pub. L. 98-94, title XII, § 1268(2), Sept. 24, 1983, 97 Stat. 705; renumbered § 127 and amended Pub. L. 99-433, title I, §§ 101(a)(3), 110(d)(4), Oct. 1, 1986, 100 Stat. 994, 1002.)

AMENDMENTS

1986—Pub. L. 99-433 renumbered section 140 of this title as this section and substituted "Emergency" for "Emergencies" in section catchline.

1983—Subsec. (a). Pub. L. 98-94 struck out "of this section" after "subsection (c)".

Subsec. (c). Pub. L. 98-94 struck out "of this section" after "subsections (a) and (b)".

CONSTRUCTION AUTHORITY OF SECRETARY OF DEFENSE UNDER DECLARATION OF WAR OR NATIONAL EMERGENCY

Pub. L. 97-99, title IX, § 903, Dec. 23, 1981, 95 Stat. 1382, which authorized the Secretary of Defense, in the event of a declaration of war or the declaration of a national emergency by the President, to undertake military construction without regard to any other provisions of law, was repealed and reenacted as section 2808 of this title by Pub. L. 97-214, §§ 2(a), 7(18), July 12, 1982, 96 Stat. 157, 174, effective Oct. 1, 1982.

§ 128. Physical protection of special nuclear material: limitation on dissemination of unclassified information

(a)(1) In addition to any other authority or requirement regarding protection from dissemination of information, and subject to section 552(b)(3) of title 5, the Secretary of Defense, with respect to special nuclear materials, shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material.

(2) The Secretary may prescribe regulations or issue orders under paragraph (1) to prohibit the dissemination of any information described in such paragraph only if and to the extent that the Secretary determines that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(A) illegal production of nuclear weapons, or

(B) theft, diversion, or sabotage of special nuclear materials, equipment, or facilities.

(3) In making a determination under paragraph (2), the Secretary may consider what the likelihood of an illegal production, theft, diversion, or sabotage referred to in such paragraph would be if the information proposed to be prohibited from dissemination under this section were at no time available for dissemination.

(4) The Secretary shall exercise his authority under this subsection to prohibit the dissemination of any information described in paragraph (1)—

(A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security; and

(B) upon a determination that the unauthorized dissemination of such information could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(i) illegal production of nuclear weapons, or

(ii) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(b) Nothing in this section shall be construed to authorize the Secretary to withhold, or to authorize the withholding of, information from the appropriate committees of the Congress.

(c) Any determination by the Secretary concerning the applicability of this section shall be subject to judicial review pursuant to section 552(a)(4)(B) of title 5.

(d) The Secretary shall prepare on a quarterly basis a report to be made available upon the request of any interested person, detailing the Secretary's application during that period of each regulation or order prescribed or issued under this section. In particular, such report shall—

(1) identify any information protected from disclosure pursuant to such regulation or order;

(2) specifically state the Secretary's justification for determining that unauthorized dissemination of the information protected from disclosure under such regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of illegal production of nuclear weapons or the theft, diversion, or sabotage of special nuclear materials, equipment, or facilities, as specified under subsection (a); and

(3) provide justification that the Secretary has applied such regulation or order so as to protect from disclosure only the minimum amount of information necessary to protect the health and safety of the public or the common defense and security.

(Added Pub. L. 100-180, div. A, title XI, § 1123(a), Dec. 4, 1987, 101 Stat. 1149.)

PRIOR PROVISIONS

A prior section 128 was renumbered section 421 of this title.

PUBLIC LAW 100-235—JAN. 8, 1988

COMPUTER SECURITY ACT OF 1987

19-139 O - 88 - (235)

Public Law 100-235
100th Congress

An Act

Jan. 8, 1988
[H.R. 145]

To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Computer Security Act of 1987.
Classified information.
40 USC 759 note.
40 USC 759 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

15 USC 272.

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

15 USC 278h.

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

15 USC 278g-3.

"SEC. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987; Regulations.

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to

devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal fur ction; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer

system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows: 15 USC 278g-4

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. Reports.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board

Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

(3) by adding at the end thereof the following new section:

National Bureau of Standards Act. 15 USC 271 note.

"SEC. 23. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

President of U.S.

Federal Register, publication.

"(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental

Federal Register, publication.

Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection. Regulations.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING. 40 USC 759 note.

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY. 40 USC 759 note.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards

and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

40 USC 759 note.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

40 USC 759 note.

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

Public information.

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Approved January 8, 1988.

LEGISLATIVE HISTORY—H.R. 145:

HOUSE REPORTS: No. 100-153, Pt. 1 (Comm. on Science, Space, and Technology) and Pt. 2 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 133 (1987):

June 22, considered and passed House.

Dec. 21, considered and passed Senate.

O

(b) The authority conferred by this section may be delegated by the Secretary of Defense to any person in the Department of Defense or by the Secretary of a military department to any person within his department, with or without the authority to make successive redelegations.

(c) In any case in which funds are expended under the authority of subsections (a) and (b), the Secretary of Defense shall submit a report of such expenditures on a quarterly basis to the Committees on Armed Services and Appropriations of the Senate and the House of Representatives.

(Added Pub. L. 94-106, title VIII, § 804(a), Oct. 7, 1975, 89 Stat. 538, § 140; amended Pub. L. 98-94, title XII, § 1268(2), Sept. 24, 1983, 97 Stat. 705; renumbered § 127 and amended Pub. L. 99-433, title I, §§ 101(a)(3), 110(d)(4), Oct. 1, 1986, 100 Stat. 994, 1002.)

AMENDMENTS

1986—Pub. L. 99-433 renumbered section 140 of this title as this section and substituted "Emergency" for "Emergencies" in section catchline.

1983—Subsec. (a), Pub. L. 98-94 struck out "of this section" after "subsection (c)".

Subsec. (c), Pub. L. 98-94 struck out "of this section" after "subsections (a) and (b)".

CONSTRUCTION AUTHORITY OF SECRETARY OF DEFENSE UNDER DECLARATION OF WAR OR NATIONAL EMERGENCY

Pub. L. 97-99, title IX, § 903, Dec. 23, 1981, 95 Stat. 1382, which authorized the Secretary of Defense, in the event of a declaration of war or the declaration of a national emergency by the President, to undertake military construction without regard to any other provisions of law, was repealed and reenacted as section 2808 of this title by Pub. L. 97-214, §§ 2(a), 7(18), July 12, 1982, 96 Stat. 157, 174, effective Oct. 1, 1982.

§ 128. Physical protection of special nuclear material: limitation on dissemination of unclassified information

(a)(1) In addition to any other authority or requirement regarding protection from dissemination of information, and subject to section 552(b)(3) of title 5, the Secretary of Defense, with respect to special nuclear materials, shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material.

(2) The Secretary may prescribe regulations or issue orders under paragraph (1) to prohibit the dissemination of any information described in such paragraph only if and to the extent that the Secretary determines that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(A) illegal production of nuclear weapons, or

(B) theft, diversion, or sabotage of special nuclear materials, equipment, or facilities.

(3) In making a determination under paragraph (2), the Secretary may consider what the likelihood of an illegal production, theft, diversion, or sabotage referred to in such paragraph would be if the information proposed to be prohibited from dissemination under this section were at no time available for dissemination.

(4) The Secretary shall exercise his authority under this subsection to prohibit the dissemination of any information described in paragraph (1)—

(A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security; and

(B) upon a determination that the unauthorized dissemination of such information could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(i) illegal production of nuclear weapons, or

(ii) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(b) Nothing in this section shall be construed to authorize the Secretary to withhold, or to authorize the withholding of, information from the appropriate committees of the Congress.

(c) Any determination by the Secretary concerning the applicability of this section shall be subject to judicial review pursuant to section 552(a)(4)(B) of title 5.

(d) The Secretary shall prepare on a quarterly basis a report to be made available upon the request of any interested person, detailing the Secretary's application during that period of each regulation or order prescribed or issued under this section. In particular, such report shall—

(1) identify any information protected from disclosure pursuant to such regulation or order;

(2) specifically state the Secretary's justification for determining that unauthorized dissemination of the information protected from disclosure under such regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of illegal production of nuclear weapons or the theft, diversion, or sabotage of special nuclear materials, equipment, or facilities, as specified under subsection (a); and

(3) provide justification that the Secretary has applied such regulation or order so as to protect from disclosure only the minimum amount of information necessary to protect the health and safety of the public or the common defense and security.

(Added Pub. L. 100-180, div. A, title XI, § 1123(a), Dec. 4, 1987, 101 Stat. 1149.)

PRIOR PROVISIONS

A prior section 128 was renumbered section 421 of this title.

CENTRAL INTELLIGENCE AGENCY ACT OF 1949

ACT OF JUNE 20, 1949

AN ACT To provide for the administration of the Central Intelligence Agency, established pursuant to section 102, National Security Act of 1947, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

DEFINITIONS

SECTION 1. [50 U.S.C. 403a] That when used in this Act, the term—

(a) "Agency" means the Central Intelligence Agency;

(b) "Director" means the Director of Central Intelligence;

(c) "Government agency" means any executive department, commission, council, independent establishment, corporation wholly or partly owned by the United States which is an instrumentality of the United States, board, bureau, division, service, office, officer, authority, administration, or other establishment, in the executive branch of the Government.

SEAL OF OFFICE

SEC. 2. [50 U.S.C. 403b] The Director of Central Intelligence shall cause a seal of office to be made for the Central Intelligence Agency, of such design as the President shall approve, and judicial notice shall be taken thereof.

PROCUREMENT AUTHORITIES

SEC. 3. [50 U.S.C. 403c] (a) In the performance of its functions the Central Intelligence Agency is authorized to exercise the authorities contained in sections 2(c) (1), (2), (3), (4), (5), (6), (10), (12), (15), (17), and sections 3, 4, 5, 6, and 10 of the Armed Services Procurement Act of 1947[1] (Public Law 413, Eightieth Congress, second session).

(b) In the exercise of the authorities granted in subsection (a) of this section, the term "Agency head" shall mean the Director, the Deputy Director, or the Executive of the Agency.

(c) The determinations and decisions provided in subsection (a) of this section to be made by the Agency head may be made with respect to individual purchases and contracts or with respect to class-

[1] The Armed Services Procurement Act of 1947 was repealed by the law enacting titles 10 and 32, United States Code (Act of August 10, 1956, 70A Stat. 1). The cited sections were replaced by sections 2304(a) (1)-(6), (10), (12), (15), and (17), 2305 (a)-(c), 2306, 2307, 2308, 2309, 2312, and 2313 of title 10. Section 49(b) of that Act provided: "References that other laws, regulations, and orders make to the replaced law shall be considered to be made to the corresponding provisions of [the sections enacting titles 10 and 32]."

es of purchases or contracts, and shall be final. Except as provided in subsection (d) of this section, the Agency head is authorized to delegate his powers provided in this section, including the making of such determinations and decisions, in his discretion and subject to his direction, to any other officer or officers or officials of the Agency.

(d) The power of the Agency head to make the determinations or decisions specified in paragraphs (12) and (15) of section 2(c) and section 5(a) of the Armed Services Procurement Act of 1947 [2] shall not be delegable. Each determination or decision required by paragraphs (12) and (15) of section 2(c), by section 4 or by section 5(a) of the Armed Services Procurement Act of 1947,[3] shall be based upon written findings made by the official making such determinations, which findings shall be final and shall be available within the Agency for a period of at least six years following the date of the determination.

(e) Notwithstanding subsection (e) of section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(e)), the provisions of section 111 of such Act relating to the procurement of automatic data processing equipment or services shall not apply with respect to such procurement by the Central Intelligence Agency.[3a]

[Original section 4 (50 U.S.C. 403d) was repealed by section 21(b)(2) of Public Law 85-507 (72 Stat. 337, July 7, 1958).]

TRAVEL, ALLOWANCES, AND RELATED EXPENSES

SEC. 4. [50 U.S.C. 403e] (a) Under such regulations as the Director may prescribe, the Agency, with respect to its officers and employees assigned to duty stations outside the several States of the United States of America, excluding Alaska and Hawaii, but including the District of Columbia, shall—

(1)(A) pay the travel expenses of officers and employees of the Agency, including expenses incurred while traveling pursuant to authorized home leave;

(B) pay the travel expenses of members of the family of an officer or employee of the Agency when proceeding to or returning from his post of duty; accompanying him on authorized home leave; or otherwise traveling in accordance with authority granted pursuant to the terms of this or any other Act;

(C) pay the cost of transporting the furniture and household and personal effects of an officer or employee of the Agency to his successive posts of duty and, on the termination of his services, to his residence at time of appointment or to a point not more distant, or, upon retirement, to the place where he will reside;

(D) pay the cost of packing and unpacking, transporting to and from a place of storage, and storing the furniture and

[2] See footnote 1. The cited provisions were replaced by paragraphs (12) and (15) of section 2304(a) and section 2307(a) of title 10.

[3] See footnote 1. The cited provisions were replaced by paragraphs (12) and (15) of section 2304(a), section 2306 and 2313, and section 2307(a) of title 10.

[3a] Public Law 97-269 provided that subsection (e) of section 8 of the Central Intelligence Agency Act of 1949 does not apply to a contract made before September 27, 1982.

household and personal effects of an officer or employee of the Agency, when he is absent from his post of assignment under orders, or when he is assigned to a post to which he cannot take or at which he is unable to use such furniture and household and personal effects, or when it is in the public interest or more economical to authorize storage; but in no instance shall the weight or volume of the effects stored together with the weight or volume of the effects transported exceed the maximum limitations fixed by regulations, when not otherwise fixed by law;

(E) pay the cost of packing and unpacking, transporting to and from a place of storage, and storing the furniture and household and personal effects of an officer or employee of the Agency in connection with assignment or transfer to a new post, from the date of his departure from his last post or from the date of his departure from his place of residence in the case of a new officer or employee and for not to exceed three months after arrival at the new post, or until the establishment of residence quarters, whichever shall be shorter; and in connection with separation of an officer or employee of the Agency, the cost of packing and unpacking, transporting to and from a place of storage, and storing for a period not to exceed three months, his furniture and household and personal effects; but in no instance shall the weight or volume of the effects stored together with the weight or volume of the effects transported exceed the maximum limitations fixed by regulations, when not otherwise fixed by law.

(F) pay the travel expenses and transportation costs incident to the removal of the members of the family of an officer or employee of the Agency and his furniture and household and personal effects, including automobiles, from a post at which, because of the prevalence of disturbed conditions, there is imminent danger to life and property, and the return of such persons, furniture, and effects to such post upon the cessation of such conditions; or to such other post as may in the meantime have become the post to which such officer or employee has been assigned.

(2) Charge expenses in connection with travel of personnel, their dependents, and transportation of their household goods and personal effects, involving a change of permanent station, to the appropriation for the fiscal year current when any part of either the travel or transportation pertaining to the transfer begins pursuant to previously issued travel and transfer orders, notwithstanding the fact that such travel or transportation may not all be effected during such fiscal year, or the travel and transfer orders may have been issued during the prior fiscal year.

(3)(A) Order to any of the several States of the United States of America (including the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States) on leave of absence each officer or employee of the Agency who was a resident of the United States (as described above) at time of employment, upon completion of two

years' continuous service abroad, or as soon as possible thereafter.

(B) While in the United States (as described in paragraph (3)(A) of this section) on leave, the service of any officer or employee shall be available for work or duties in the Agency or elsewhere as the Director may prescribe; and the time of such work or duty shall not be counted as leave.

(C) Where an officer or employee on leave returns to the United States (as described in paragraph (3)(A) of this section), leave of absence granted shall be exclusive of the time actually and necessarily occupied in going to and from the United States (as so described) and such time as may be necessarily occupied in awaiting transportation.

(4) Notwithstanding the provisions of any other law, transport for or on behalf of an officer or employee of the Agency, a privately owned motor vehicle in any case in which it shall be determined that water, rail, or air transportation of the motor vehicle is necessary or expedient for all or any part of the distance between points of origin and destination, and pay the costs of such transportation. Not more than one motor vehicle of any officer or employee of the Agency may be transported under authority of this paragraph during any four-year period, except that, as replacement for such motor vehicle, one additional motor vehicle of any such officer or employee may be so transported during such period upon approval, in advance, by the Director and upon a determination, in advance, by the Director that such replacement is necessary for reasons beyond the control of the officer or employee and is in the interest of the Government. After the expiration of a period of four years following the date of transportation under authority of this paragraph of a privately owned motor vehicle of any officer or employee who has remained in continuous service outside the several States of the United States of America, excluding Alaska and Hawaii, but including the District of Columbia, during such period, the transportation of a replacement for such motor vehicle for such officer or employee may be authorized by the Director in accordance with this paragraph.

(5) (A) In the event of illness or injury requiring the hospitalization of an officer or full time employee of the Agency, not the result of vicious habits, intemperance, or misconduct on his part, incurred while on assignment abroad, in a locality where there does not exist a suitable hospital or clinic, pay the travel expenses of such officer or employee by whatever means he shall deem appropriate and without regard to the Standardized Government Travel Regulations and section 10 of the Act of March 3, 1933 [4] (47 Stat. 1516; 5 U.S.C. 73b), to the nearest locality where a suitable hospital or clinic exists and on his recovery pay for the travel expenses of his return to his post of

[4] The cited Act of March 3, 1933, was repealed by the law enacting title 5, United States Code (Public Law 89-544, Sept. 6, 1966, 80 Stat. 378). Section 10 of that act was codified as section 5731(a) of title 5. Section 7(b) of Public Law 89-544 (80 Stat. 631) provided: "A reference to a law replaced by sections 1-6 of this Act, including a reference in a regulation, order, or other law, is deemed to refer to the corresponding provision enacted by this Act."

duty. If the officer or employee is too ill to travel unattended the Director may also pay the travel expenses of an attendant.

(B) Establish a first-aid station and provide for the service of a nurse at a post at which, in his opinion, sufficient personnel is employed to warrant such a station: *Provided*, That, in his opinion, it is not feasible to utilize an existing facility;

(C) In the event of illness or injury requiring hospitalization of an officer or full time employee of the Agency, not the result of vicious habits, intemperance, or misconduct on his part, incurred in the line of duty while such person is assigned abroad, pay for the cost of the treatment of such illness or injury at a suitable hospital or clinic;

(D) Provide for the periodic physical examination of officers and employees of the Agency and for the cost of administering inoculations or vaccinations to such officers or employees.

(6) Pay the costs of preparing and transporting the remains of an officer or employee of the Agency or a member of his family who may die while in travel status or abroad, to his home or official station, or to such other place as the Director may determine to be the appropriate place of interment, provided that in no case shall the expense payable be greater than the amount which would have been payable had the destination been the home or official station.

(7) Pay the costs of travel of new appointees and their dependents, and the transportation of their household goods and personal effects, from places of actual residence in foreign countries at time of appointment to places of employment and return to their actual residences at the time of appointment or a point not more distant: *Provided*, That such appointees agree in writing to remain with the United States Government for a period of not less than twelve months from the time of appointment.

Violation of such agreement for personal convenience of an employee or because of separation for misconduct will bar such return payments and, if determined by the Director or his designee to be in the best interests of the United States, any money expended by the United States on account of such travel and transportation shall be considered as a debt due by the individual concerned to the United States.

(b)(1) The Director may pay to officers and employees of the Agency, and to persons detailed or assigned to the Agency from other agencies of the Government or from the Armed Forces, allowances and benefits comparable to the allowances and benefits authorized to be paid to members of the Foreign Service under chapter 9 of title I of the Foreign Service Act of 1980 (22 U.S.C. 4081 et seq.) or any other provision of law.

(2) The Director may pay allowances and benefits related to officially authorized travel, personnel and physical security activities, operational activities, and cover-related activities (whether or not such allowances and benefits are otherwise authorized under this section or any other provision of law) when payment of such allowances and benefits is necessary to meet the special requirements of work related to such activities. Payment of allowances and benefits

under this paragraph shall be in accordance with regulations prescribed by the Director. Rates for allowances and benefits under this paragraph may not be set at rates in excess of those authorized by section 5724 and 5724a of title 5, United States Code, when reimbursement is provided for relocation attributable, in whole or in part, to relocation within the United States.

(3) Notwithstanding any other provision of this section or any other provision of law relating to the officially authorized travel of Government employees, the Director, in order to reflect Agency requirements not taken into account in the formulation of Government-wide travel procedures, may by regulation—

(A) authorize the travel of officers and employees of the Agency, and of persons detailed or assigned to the Agency from other agencies of the Government or from the Armed Forces who are engaged in the performance of intelligence functions, and

(B) provide for payment for such travel, in classes of cases, as determined by the Director, in which such travel is important to the performance of intelligence functions.

(4) Members of the Armed Forces may not receive benefits under both this section and title 37, United States Code, for the same purpose. The Director and Secretary of Defense shall prescribe joint regulations to carry out the preceding sentence.

(5) Regulations issued pursuant to this subsection shall be submitted to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate before such regulations take effect.

GENERAL AUTHORITIES

SEC. 5. [50 U.S.C. 403f] In the performance of its functions, the Central Intelligence Agency is authorized to—

(a) Transfer to and receive from other Government agencies such sums as may be approved by the Bureau of the Budget, for the performance of any of the functions or activities authorized under sections 102 and 303 of the National Security Act of 1947 (Public Law 253, Eightieth Congress, and any other Government agency is authorized to transfer to or receive from the Agency such sums without regard to any provisions of law limiting or prohibiting transfers between appropriations. Sums transferred to the Agency in accordance with this paragraph may be expended for the purposes and under the authority of this Act without regard to limitations of appropriations from which transferred;

(b) Exchange funds without regard to section 3651 Revised Statutes (31 U.S.C. 543);

(c) Reimburse other Government agencies for services of personnel assigned to the Agency, and such other Government agencies are hereby authorized, without regard to provisions of law to the contrary, so to assign or detail any officer or employee for duty with the Agency;

(d) Authorize personnel designated by the Director to carry firearms to the extent necessary for the performance of the Agency's authorized functions, except that, within the United States, such authority shall be limited to the purposes of protection of classified

materials and information, the training of Agency personnel and other authorized persons in the use of firearms, the protection of Agency installations and property, and the protection of Agency personnel and of defectors, their families, and other persons in the United States under Agency auspices;

(e) Make alterations, improvements, and repairs on premises rented by the Agency, and pay rent therefor without regard to limitations on expenditures contained in the Act of June 30, [illegible] amended: *Provided*, That in each case the Director shall certify that exception from such limitations is necessary to the successful performance of the Agency's functions or to the security of its activities; and

(f) Determine and fix the minimum and maximum limits of age within which an original appointment may be made to an operational position within the Agency, notwithstanding the provision of any other law, in accordance with such criteria as the Director, in his discretion, may prescribe.

SEC. 6. [50 U.S.C. 403g] In the interests of the security of the foreign intelligence activities of the United States and in order further to implement the proviso of section 102(d)(3) of the National Security Act of 1947 (Public Law 253, Eightieth Congress, first session) that the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure, the Agency shall be exempted from the provisions of sections 1 and 2, chapter 795, of the Act of August 28, [illegible] (49 Stat. 956, 957; 5 U.S.C. 654) and the provisions of any other law which require the publication or disclosure of the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency: *Provided*, That in furtherance of these objectives, the Director of the Bureau of the Budget shall make such reports to the Congress in connection with the Agency under section 607, title VI, chapter 212 of the Act of June 30, 1945, as amended (5 U.S.C. 947(b)).

SEC. 7. [50 U.S.C. 403h] Whenever the Director, the Attorney General, and the Commissioner of Immigration shall determine that the entry of a particular alien into the United States for permanent residence is in the interest of national security or essential to furtherance of the national intelligence mission, such alien and his immediate family shall be given entry into the United States for permanent residence without regard to their inadmissibility under the immigration or any other laws and regulations, or failure to comply with such laws and regulations pertaining to admissibility: *Provided*, That the number of aliens and members of their immediate families entering the United States under the authority of this section shall in no case exceed one hundred per[illegible] one fiscal year.

[illegible] the Act entitled "An Act making appropriations for the Legislative Branch [illegible] for the fiscal year ending June 30, 1948, and for other purposes" (47 Stat. [illegible] of that Act relating to rental of buildings by the Government see sections [illegible] (U.S.C. 303b, 278a). See also section 210(a)(5) of the Federal Property and Administrative Act of 1949 (40 U.S.C. [illegible]).

[illegible] of August 28, 1935, was repealed by the Independent Offices Appropriation [illegible] Law 86-626, 74 Stat. [illegible]

[illegible] the Act of June 30, 1945, was repealed by section 201(85) of the Budget and Accounting Act of 1950 (64 Stat. [illegible]).

[Original section 9 (50 U.S.C. 403i) was repealed by section 601(b) of Public Law 763, 68 Stat. 1115; September 1, 1954.]

APPROPRIATIONS

SEC. 8. [50 U.S.C. 403j] (a) Notwithstanding any other provisions of law, sums made available to the Agency by appropriation or otherwise may be expended for purposes necessary to carry out its functions, including—

(1) personal services, including personal services without regard to limitations on types of persons to be employed, and rent at the seat of government and elsewhere; health-service program as authorized by law (5 U.S.C. 150) [8] rental of news-reporting services; purchase or rental and operation of photographic, reproduction, cryptographic, duplication and printing machines, equipment and devices, and radio-receiving and radio-sending equipment and devices, including telegraph and teletype equipment; purchase, maintenance, operation, repair, and hire of passenger motor vehicles, and aircraft, and vessels of all kinds; subject to policies established by the Director, transportation of officers and employees of the Agency in Government-owned automotive equipment between their domiciles and places of employment, where such personnel are engaged in work which makes such transportation necessary, and transportation in such equipment, to and from school, of children of Agency personnel who have quarters for themselves and their families at isolated stations outside the continental United States where adequate public or private transportation is not available; printing and binding; purchase, maintenance, and cleaning of firearms, including purchase, storage, and maintenance of ammunition; subject to policies established by the Director, expenses of travel in connection with and expenses incident to attendance at meetings of professional, technical, scientific, and other similar organizations when such attendance would be a benefit in the conduct of the work of the Agency; association and library dues; payment of premiums or costs of surety bonds for officers or employees without regard to the provisions of 61 Stat. 646; 6 U.S.C. 14; [9] payment of claims pursuant to 28 U.S.C.; acquisition of necessary land and the clearing of such land; construction of buildings and facilities without regard to 86 Stat. 699; 40 U.S.C. 259, 267;[10] repair, rental, operation, and maintenance of buildings, utilities, facilities, and appurtenances; and

[8] The law codified to section 150 of title 5 before the enactment of that title was replaced by section 7901 of title 5 upon the enactment of that title by Public Law 89-544 (Sept. 6, 1966, 80 Stat. 378).

[9] Section 14 of title 6, United States Code, relating to the purchase of bonds to cover Government employees, was repealed by section 203(1) of Public Law 92-310 (Act of June 6, 1972, 86 Stat. 202).

[10] Section 3734 of the Revised Statutes of the United States, formerly classified to sections 259 and 267 of title 40, was repealed by section 17(12) of the Public Buildings Act of 1959 (Public Law 86-249, 73 Stat. 485). That Act is shown in the United States Code as chapter 12 of title 40 (40 U.S.C. 601 et seq.).

(2) supplies, equipment, and personnel and contractual services otherwise authorized by law and regulations, when approved by the Director.

(b) The sums made available to the Agency may be expended without regard to the provisions of law and regulations relating to the expenditure of Government funds; and for objects of a confidential, extraordinary, or emergency nature, such expenditures to be accounted for solely on the certificate of the Director and every such certificate shall be deemed a sufficient voucher for the amount therein certified.

SEPARABILITY OF PROVISIONS

SEC. 9. [50 U.S.C. 403a note] If any provision of this Act, or the application of such provision to any person or circumstances, is held invalid, the remainder of this Act or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected thereby.

SHORT TITLE

SEC. 10. [50 U.S.C. 401 note] This Act may be cited as the "Central Intelligence Agency Act of 1949".

AUTHORITY TO PAY DEATH GRATUITIES

SEC. 11. [50 U.S.C. 403k] (a)(1) The Director may pay a gratuity to the surviving dependents of any officer or employee of the Agency who dies as a result of injuries (other than from disease) sustained outside the United States and whose death—

(A) resulted from hostile or terrorist activities; or

(B) occurred in connection with an intelligence activity having a substantial element of risk.

(2) The provisions of this subsection shall apply with respect to deaths occurring after June 30, 1974.

(b) Any payment under subsection (a)—

(1) shall be in an amount equal to the amount of the annual salary of the officer or employee concerned at the time of death;

(2) shall be considered a gift and shall be in lieu of payment of any lesser death gratuity authorized by any other Federal law; and

(3) shall be made under the same conditions as apply to payments authorized by section 14 of the Act of August 1, 1956 (22 U.S.C. 2679a).[11]

AUTHORITY TO ACCEPT GIFTS, DEVISES, AND BEQUESTS

SEC. 12. [50 U.S.C. 403l] (a) Subject to the provisions of this section, the Director may accept, hold, administer, and use gifts of

[11] Section 14 of the Act of August 1, 1956, was repealed effective February 15, 1981, by section [illegible] of the Foreign Service Act of 1980 (Public Law 96-465, 94 Stat. 2160). The subject of [illegible] for Foreign Service employees is now covered by section 418 of that Act (22 [illegible] 94 Stat. 2092). Section 2401(c) of that Act (94 Stat. 2168) provided: "References in [illegible] of the Foreign Service Act of 1946 or other law superseded by that Act shall be [illegible] to include reference to the corresponding provisions of this Act.".

money, securities, or other property whenever the Director determines it would be in the interest of the United States to do so. Any gift accepted under this section (and any income produced by any such gift) may be used only for artistic display or for purposes relating to the general welfare, education, or recreation of employees or dependents of employees of the Agency or for similar purposes, and under no circumstances may such a gift (or any income produced by any such gift) be used for operational purposes. The Director may not accept any gift under this section which is expressly conditioned upon any expenditure not to be met from the gift itself or from income produced by the gift unless such expenditure has been authorized by law.

(b) Unless otherwise restricted by the terms of the gift, the Director may sell or exchange, or invest or reinvest, any property which is accepted under this section, but any such investment may only be in interest-bearing obligations of the United States or in obligations guaranteed as to both principal and interest by the United States.

(c) There is hereby created on the books of the Treasury of the United States a fund into which gifts of money, securities, and other intangible property accepted under the authority of this section, and the earnings and proceeds thereof, shall be deposited. The assets of such fund shall be disbursed upon the order of the Director for the purposes specified in subsection (a) or (b).

(d) For purposes of Federal income, estate, and gift taxes, gifts accepted by the Director under this section shall be considered to be to or for the use of the United States.

(e) For the purposes of this section, the term "gift" includes a bequest or devise.

MISUSE OF AGENCY NAME, INITIALS OR SEAL

SEC. 13. [50 U.S.C. 403m] (a) No person may, except with the written permission of the Director, knowingly use the words 'Central Intelligence Agency', the initials 'CIA', the seal of the Central Intelligence Agency, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Central Intelligence Agency.

(b) Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

RETIREMENT EQUITY FOR SPOUSES OF CERTAIN EMPLOYEES

SEC. 14. [50 U.S.C. 403n] (a) The provisions of sections 204, 221(b)(1)–(3), 221(f), 221(g)(2), 221(l), 221(m), 221(n), 221(o), 222, 223, 224, 234(c), 234(d), 234(e), and 263(b) of the Central Intelligence Agency Retirement Act of 1964 for Certain Employees (50 U.S.C. 403 note) establishing certain requirements, limitations, rights, entitlements, and benefits relating to retirement annuities, survivor benefits, and lump-sum payments for a spouse or former spouse of an Agency employee who is a participant in the Central Intelligence Agency Retirement and Disability System shall apply in the same manner and to the same extent in the case of an Agency employee who is a participant in the Civil Service Retirement and Disability System.

(b) The Director of the Office of Personnel Management, in consultation with the Director of Central Intelligence, shall prescribe such regulations as may be necessary to implement the provisions of this section.

SECURITY PERSONNEL AT AGENCY INSTALLATIONS

SEC. 15. [50 U.S.C. 403o] (a) The Director may authorize Agency personnel within the United States to perform the same functions as special policemen of the General Services Administration perform under the first section of the Act entitled "An Act to authorize the Federal Works Administrator or officials of the Federal Works Agency duly authorized by him to appoint special policemen for duty upon Federal property under the jurisdiction of the Federal Works Agency, and for other purposes" (40 U.S.C. 318), with the powers set forth in that section, except that such personnel shall perform such functions and exercise such powers only within Agency installations, and the rules and regulations enforced by such personnel shall be rules and regulations promulgated by the Director.

(b) The Director is authorized to establish penalties for violations of the rules or regulations promulgated by the Director under subsection (a) of this section. Such penalties shall not exceed those specified in the fourth section of the Act referred to in subsection (a) of this section (40 U.S.C. 318c).

(c) Agency personnel designated by the Director under subsection (a) of this section shall be clearly identifiable as United States Government security personnel while engaged in the performance of the functions to which subsection (a) of this section refers.

HEALTH BENEFITS FOR CERTAIN FORMER SPOUSES OF CENTRAL INTELLIGENCE AGENCY EMPLOYEES

SEC. 16. [50 U.S.C. 403p] (a) Except as provided in subsection (d)(1), any individual—

(1) formerly married to an employee or former employee of the Agency, whose marriage was dissolved by divorce or annulment before May 7, 1985;

(2) who, at any time during the eighteen-month period before the divorce or annulment became final, was covered under a

CENTRAL INTELLIGENCE AGENCY RETIREMENT ACT OF 1964 FOR CERTAIN EMPLOYEES

PUBLIC LAW 88-643—OCTOBER 13, 1964

(50 U.S.C. 403 note)

AN ACT To provide for the establishment and maintenance of a Central Intelligence Agency Retirement and Disability System for a limited number of employees, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I—TITLE AND DEFINITIONS

PART A—TITLE

SEC. 101. This Act may be cited as the "Central Intelligence Agency Retirement Act of 1964 for Certain Employees".

PART B—DEFINITIONS

SEC. 111. When used in this Act, the term—

(1) "Agency" means the Central Intelligence Agency;

(2) "Director" means the Director of Central Intelligence;

(3) "Qualifying service" means service performed as a participant in the system or, in the case of service prior to designation, service determined by the Director to have been performed in carrying out duties described in section 203;

(4) "Fund balance" means the sum of—

(a) the investments of the fund calculated at par value; and

(b) the cash balance of the fund on the books of the Treasury;

(5) "Unfunded liability" means the estimated excess of the present value of all benefits payable from the fund to participants and former participants, subject to this Act, and to their survivors, over the sum of—

(a) the present value of deductions to be withheld from the future basic salary of participants currently subject to this Act and of future Agency contributions to be made in their behalf; plus

(b) the present value of Government payments to the fund under section 261 (b) and (c) of this Act; plus

(c) the fund balance as of the date the unfunded liability is determined; and

(6) "Normal cost" means the level percentage of payroll required to be deposited in the fund to meet the cost of benefits payable under the system (computed in accordance with generally accepted actuarial practice on an entry-age basis) less the

dustrial design, or model in respect of the invention. A United States patent issued to such person, his successors, assigns, or legal representatives shall be invalid.

§ 186. Penalty

Whoever, during the period or periods of time an invention has been ordered to be kept secret and the grant of a patent thereon withheld pursuant to section 181 of this title, shall, with knowledge of such order and without due authorization, willfully publish or disclose or authorize or cause to be published or disclosed the invention, or material information with respect thereto, or whoever, in violation of the provisions of section 184 of this title, shall file or cause or authorize to be filed in any foreign country an application for patent or for the registration of a utility model, industrial design, or model in respect of any invention made in the United States, shall, upon conviction, be fined not more than $10,000 or imprisoned for not more than two years, or both.

§ 187. Nonapplicability to certain persons

The prohibitions and penalties of this chapter shall not apply to any officer or agent of the United States acting within the scope of his authority, nor to any person acting upon his written instructions or permission.

§ 188. Rules and regulations, delegation of power [1]

The Atomic Energy Commission, the Secretary of a defense department, the chief officer of any other department or agency of the Government designated by the President as a defense agency of the United States, and the Secretary of Commerce, may separately issue rules and regulations to enable the respective department or agency to carry out the provisions of this chapter, and may delegate any power conferred by this chapter.

CHAPTERS 12 AND 18 OF THE ATOMIC ENERGY ACT OF 1954 (PROTECTION OF ATOMIC ENERGY INFORMATION)[2]

CHAPTER 2. DEFINITIONS

SEC. 11. [42 U.S.C. 2014] DEFINITIONS.—The intent of Congress in the definitions as given in this section should be construed from the words or phrases used in the definitions. As used in this Act:

a. The term "agency of the United States" means the executive branch of the United States, or any Government agency, or the legislative branch of the United States, or any agency, committee, commission, office, or other establishment in the legislative branch, or the judicial branch of the United States, or any office, agency,

---

[1] See footnotes 3 and 4, ante.

[2] Throughout the Atomic Energy Act of 1954, the term "Commission" means the Atomic Energy Commission. The functions of the Atomic Energy Commission, which previously were transferred to the Administrator of the Energy Research and Development Administration, were transferred to the Secretary of Energy by section 301 of the Department of Energy Organization Act (Public Law 95-91; 91 Stat. 577).

committee, commission, or other establishment in the judicial branch.

• • • • • • •

h. The term "defense information" means any information in any category determined by any Government agency authorized to classify information, as being information respecting, relating to, or affecting the national defense.

• • • • • • •

l. The term "Government agency" means any executive department, commission, independent establishment, corporation, wholly or partly owned by the United States of America which is an instrumentality of the United States, or any board, bureau, division, service, office, officer, authority, administration, or other establishment in the executive branch of the Government.

• • • • • • •

s. The term "person" means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, Government agency other than the Commission, any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing.

• • • • • • •

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.

• • • • • • •

CHAPTER 12. CONTROL OF INFORMATION

SEC. 141. [42 U.S.C. 2161] POLICY.—It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. Consistent with such policy, the Commission shall be guided by the following principles:

a. Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 144; and

b. The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information.

SEC. 142. [42 U.S.C. 2162] 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 of the common defense and security and shall thereupon cause such data to be declassified and removed from the category of the 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.

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.

SEC. 143. [42 U.S.C. 2163] DEPARTMENT OF DEFENSE PARTICIPATION.—The Commission may authorize any of its employees, or employees of any contractor, prospective contractor, licensee or prospective licensee of the Commission or any other person authorized access to Restricted Data by the Commission under subsections 145 b. and 145 c. to permit any employee of an agency of the Department of Defense or of its contractors, or any member of the Armed Forces to have access to Restricted Data required in the performance of his duties and so certified by the head of the appropriate agency of the Department of Defense or his designee: *Provided, however,* That the head of the appropriate agency of the Department of Defense or his designee has determined, in accordance with the established personnel security procedures and standards of such agency, that permitting the member or employee to have access to such Restricted Data will not endanger the common de-

fense and security: *And provided further,* That the Secretary of Defense finds that the established personnel and other security procedures and standards of such agency are adequate and in reasonable conformity to the standards established by the Commission under section 145.

SEC. 144. [42 U.S.C. 2164] INTERNATIONAL COOPERATION.—

a. The President may authorize the Commission to cooperate with another nation and to communicate to that nation Restricted Data on—

(1) refining, purification, and subsequent treatment of source material;

(2) civilian reactor development;

(3) production of special nuclear material;

(4) health and safety;

(5) industrial and other applications of atomic energy for peaceful purposes; and

(6) research and development relating to the foregoing:

Provided, however, That no such cooperation shall involve the communication of Restricted Data relating to the design or fabrication of atomic weapons: *And provided further,* That the cooperation is undertaken pursuant to an agreement for cooperation entered into in accordance with section 123, or is undertaken pursuant to an agreement existing on the effective date of this Act.

b. The President may authorize the Department of Defense, with the assistance of the Commission, to cooperate with another nation or with a regional defense organization to which the United States is a party, and to communicate to that nation or organization such Restricted Data (including design information) as is necessary to—

(1) the development of defense plans;

(2) the training of personnel in the employment of and defense against atomic weapons and other military applications of atomic energy;

(3) the evaluation of the capabilities of potential enemies in the employment of atomic weapons and other military applications of atomic energy; and

(4) the development of compatible delivery systems for atomic weapons;

whenever the President determines that the proposed cooperation and the proposed communication of the Restricted Data will promote and will not constitute an unreasonable risk to the common defense and security, while such other nation or organization is participating with the United States pursuant to an international arrangement by substantial and material contributions to the mutual defense and security: *Provided, however,* That the cooperation is undertaken pursuant to an agreement entered into in accordance with section 123.

c. In addition to the cooperation authorized in subsections 144 a. and 144 b., the President may authorize the Commission, with the assistance of the Department of Defense, to cooperate with another nation and—

(1) to exchange with that nation Restricted Data concerning atomic weapons: *Provided,* That communication of such Restricted Data to that nation is necessary to improve its atomic weapon design, development, or fabrication capability and provided that nation has made substantial progress in the development of atomic weapons; and

(2) to communicate or exchange with that nation Restricted Data concerning research, development, or design, of military reactors.

whenever the President determines that the proposed cooperation and the communication of the proposed Restricted Data will promote and will not constitute an unreasonable risk to the common defense and security, while such other nation is participating with the United States pursuant to an international arrangement by substantial and material contributions to the mutual defense and security: *Provided, however,* That the cooperation is undertaken pursuant to an agreement entered into in accordance with section 123.

d. The President may authorize any agency of the United States to communicate in accordance with the terms and conditions of an agreement for cooperation arranged pursuant to subsection 144 a., b., or c., such Restricted Data as is determined to be transmissible under the agreement for cooperation involved.

SEC. 145. [42 U.S.C. 2165] RESTRICTIONS.—

a. No arrangement shall be made under section 31, no contract shall be made or continued in effect under section 41, and no license shall be issued under section 103 or 104, unless the person with whom such arrangement is made, the contractor or prospective contractor, or the prospective licensee agrees in writing not to permit any individual to have access to Restricted Data until the Civil Service Commission[1] shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to Restricted Data will not endanger the common defense and security.

b. Except as authorized by the Commission or the General Manager upon a determination by the Commission or General Manager that such action is clearly consistent with the national interest, no individual shall be employed by the Commission nor shall the Commission permit any individual to have access to Restricted Data until the Civil Service Commission[1] shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

c. In lieu of the investigation and report to be made by the Civil Service Commission pursuant to subsection b. of this section, the Commission may accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individual by another Government agency based on such investigation and report.

[1] Functions of the Civil Service Commission were transferred to the Director of the Office of Personnel Management by section 102 of Reorganization Plan No. 2 of 1978 (92 Stat. 3783; 5 U.S.C. 1101 note).

d. In the event an investigation made pursuant to subsection a. and b. of this section develops any data reflecting that the individual who is the subject of the investigation is of questionable loyalty, the Civil Service Commission shall refer the matter to the Federal Bureau of Investigation for the conduct of a full field investigation, the results of which shall be furnished to the Civil Service Commission for its information and appropriate action.

e. If the President deems it to be in the national interest he may from time to time determine that investigations of any group or class which are required by subsections a., b., and c. of this section be made by the Federal Bureau of Investigation.

f. Notwithstanding the provisions of subsections a., b., and c., of this section, a majority of the members of the Commission shall certify those specific positions which are of a high degree of importance or sensitivity, and upon such certification, the investigation and reports required by such provisions shall be made by the Federal Bureau of Investigation.

g. The Commission shall establish standards and specifications in writing as to the scope and extent of investigations, the reports of which will be utilized by the Commission in making the determination, pursuant to subsections a., b., and c. of this section, that permitting a person access to restricted data will not endanger the common defense and security. Such standards and specifications shall be based on the location and class or kind of work to be done, and shall, among other considerations, take into account the degree of importance to the common defense and security of the restricted data to which access will be permitted.

h. Whenever the Congress declares that a state of war exists, or in the event of a national disaster due to enemy attack, the Commission is authorized during the state of war or period of national disaster due to enemy attack to employ individuals and to permit individuals access to Restricted Data pending the investigation report, and determination required by section 145 b., to the extent that and so long as the Commission finds that such action is required to prevent impairment of its activities in furtherance of the common defense and security.

SEC. 146. [42 U.S.C. 2166] GENERAL PROVISIONS.—

a. Sections 141 to 145, inclusive, shall not exclude the applicable provisions of any other laws, except that no Government agency shall take any action under such other laws inconsistent with the provisions of those sections.

b. The Commission shall have no power to control or restrict the dissemination of information other than as granted by this or any other law.

SEC. 147. [42 U.S.C. 2167] SAFEGUARDS INFORMATION.—

a. In addition to any other authority or requirement regarding protection from disclosure of information, and subject to subsection (b)(3) of section 552 of title 5 of the United States Code, the Commission shall prescribe such regulations, after notice and opportunity for public comment, or issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information which specifically identifies a licensee's or applicant's detailed—

(1) control and accounting procedures or security mea (including security plans, procedures, and equipment) fo physical protection of special nuclear material, by whon possessed, whether in transit or at fixed sites, in quantitie termined by the Commission to be significant to the p health and safety or the common defense and security;

(2) security measures (including security plans, proced and equipment) for the physical protection of source mat or byproduct material, by whomever possessed, whethe transit or at fixed sites, in quantities determined by the C mission to be significant to the public health and safety or common defense and security; or

(3) security measures (including security plans, procedu and equipment) for the physical protection of and the loca of certain plant equipment vital to the safety of productior utilization facilities involving nuclear materials covered paragraphs (1) and (2)

if the unauthorized disclosure of such information could reasona be expected to have a significant adverse effect on the health a safety of the public or the common defense and security by sign cantly increasing the likelihood of theft, diversion, or sabotage such material or such facility. The Commission shall exercise authority of this subsection—

(A) so as to apply the minimum restrictions needed to p tect the health and safety of the public or the common defen and security, and

(B) upon a determination that the unauthorized disclosure such information could reasonably be expected to have a sign icant adverse effect on the health and safety of the public the common defense and security by significantly increasi the likelihood of theft, diversion, or sabotage of such materi or such facility.

Nothing in this Act shall authorize the Commission to prohib the public disclosure of information pertaining to the routes an quantities of shipments of source material, by-product materia high level nuclear waste, or irradiated nuclear reactor fuel. An person, whether or not a licensee of the Commission, who violate any regulation adopted under this section shall be subject to th civil monetary penalties of section 234 of the Act. Nothing in thi section shall be construed to authorize the withholding of informa tion from the duly authorized committees of the Congress.

b. For the purposes of section 223 of this Act, any regulations o orders prescribed or issued by the Commission under this section shall also be deemed to be prescribed or issued under section 161 b of this Act.

c. Any determination by the Commission concerning the applicability of this section shall be subject to judicial review pursuant to subsection (a)(4)(B) of section 552 of title 5 of the United States Code.

d. Upon prescribing or issuing any regulation or order under subsection a. of this section, the Commission shall submit to Congress a report that:

(1) specifically identifies the type of information the Commission intends to protect from disclosure under the regulation or order;

(2) specifically states the Commission's justification for determining that unauthorized disclosure of the information to be protected from disclosure under the regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility, as specified under subsection (a) of this section; and

(3) provides justification, including proposed alternative regulations or orders, that the regulation or order applies only the minimum restrictions needed to protect the health and safety of the public or the common defense and security.

e. In addition to the reports required under subsection d. of this section, the Commission shall submit to Congress on a quarterly basis a report detailing the Commission's application during that period of every regulation or order prescribed or issued under this section. In particular, the report shall:

(1) identify any information protected from disclosure pursuant to such regulation or order;

(2) specifically state the Commission's justification for determining that unauthorized disclosure of the information protected from disclosure under such regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion or sabotage of such material or such facility, as specified under subsection a. of this section; and

(3) provide justification that the Commission has applied such regulation or order so as to protect from disclosure only the minimum amount of information necessary to protect the health and safety of the public or the common defense and security.

SEC. 148. [42 U.S.C. 2168] PROHIBITION AGAINST THE DISSEMINATION OF CERTAIN UNCLASSIFIED INFORMATION—

a. (1) In addition to any other authority or requirement regarding protection from dissemination of information, and subject to section 552(b)(3) of title 5, United States Code, the Secretary, with respect to atomic energy defense programs, of Energy (hereinafter in this section referred to as the "Secretary") shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to—

(A) the design of production facilities or utilization facilities;

(B) security measures (including security plans, procedures, and equipment) for the physical protection of (i) production or utilization facilities, (ii) nuclear material contained in such facilities, or (iii) nuclear material in transit; or

(C) the design, manufacture, or utilization of any atomic weapon or component if the design, manufacture, or utilization of such weapon or component was contained in any information

declassified or removed from the Restricted Data category by the Secretary (or the head of the predecessor agency of the Department of Energy) pursuant to section 142.

(2) The Secretary may prescribe regulations or issue orders under paragraph (1) to prohibit the dissemination of any information described in such paragraph only if and to the extent that the Secretary determines that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health or safety of the public or the common defense and security by significantly increasing the likelihood of (A) illegal production of nuclear weapons, or (B) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(3) In making a determination under paragraph (2) the Secretary may consider what the likelihood of an illegal production, theft, diversion, or sabotage referred to in such paragraph would be if the information proposed to be prohibited from dissemination under this section were at no time available for dissemination.

(4) The Secretary shall exercise his authority under this subsection to prohibit the dissemination of any information described in subsection a. (1)—

(A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security; and

(B) upon a determination that the unauthorized dissemination of such information could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of (i) illegal production of nuclear weapons, or (ii) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(5) Nothing in this section shall be construed to authorize the Secretary to authorize the withholding of information from the appropriate committees of the Congress.

b. (1) Any person who violates any regulation or order of the Secretary issued under this section with respect to the unauthorized dissemination of information shall be subject to a civil penalty, to be imposed by the Secretary, of not to exceed $100,000 for each such violation. The Secretary may compromise, mitigate, or remit any penalty imposed under this subsection.

(2) The provisions of subsection b. and c. of section 234 of this Act shall be applicable with respect to the imposition of civil penalties by the Secretary under this section in the same manner that such provisions are applicable to the imposition of civil penalties by the Commission under subsection a. of such section.

c. For the purposes of section 223 of this Act, any regulation prescribed or order issued by the Secretary under this section shall also be deemed to be prescribed or issued under section 161 b. of this Act.

d. Any determination by the Secretary concerning the applicability of this section shall be subject to judicial review pursuant to section 552(a)(4)(B) of title 5, United States Code.

e. The Secretary shall prepare on a quarterly basis a report to be made available upon the request of any interested person

ing the Secretary's application during that period of each regulation or order prescribed or issued under this section. In particular, such report shall—

(1) identify any information protected from disclosure pursuant to such regulation or order;

(2) specifically state the Secretary's justification for determining that unauthorized dissemination of the information protected from disclosure under such regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of illegal production of nuclear weapons, or theft, diversion, or sabotage of nuclear materials, equipment, or facilities, as specified under subsection a.; and

(3) provide justification that the Secretary has applied such regulation or order so as to protect from disclosure only the minimum amount of information necessary to protect the health and safety of the public or the common defense and security.

SEC. 149. [42 U.S.C. 2169] FINGERPRINTING FOR CRIMINAL HISTORY RECORD CHECKS.—

a. The Nuclear Regulatory Commission (in this section referred to as the "Commission") shall require each licensee or applicant for a license to operate a utilization facility under section 103 or 104 b. to fingerprint each individual who is permitted unescorted access to the facility or is permitted access to safeguards information under section 147. All fingerprints obtained by a licensee or applicant as required in the preceding sentence shall be submitted to the Attorney General of the United States through the Commission for identification and a criminal history records check. The costs of any identification and records check conducted pursuant to the preceding sentence shall be paid by the licensee or applicant. Notwithstanding any other provision of law, the Attorney General may provide all the results of the search to the Commission, and, in accordance with regulations prescribed under this section, the Commission may provide such results to the licensee or applicant submitting such fingerprints.

b. The Commission, by rule, may relieve persons from the obligations imposed by this section, upon specified terms, conditions, and periods, if the Commission finds that such action is consistent with its obligations to promote the common defense and security and to protect the health and safety of the public.

c. For purposes of administering this section, the Commission shall prescribe, subject to public notice and comment, regulations—

(1) to implement procedures for the taking of fingerprints;

(2) to establish the conditions for use of information received from the Attorney General, in order—

(A) to limit the redissemination of such information;

(B) to ensure that such information is used solely for the purpose of determining whether an individual shall be permitted unescorted access to the facility of a licensee or applicant or shall be permitted access to safeguards information under section 147;

(C) to ensure that no final determination may be made solely on the basis of information provided under this section involving—

(i) an arrest more than 1 year old for which there is no information of the disposition of the case; or

(ii) an arrest that resulted in dismissal of the charge or an acquittal; and

(D) to protect individuals subject to fingerprinting under this section from misuse of the criminal history record; and

(3) to provide each individual subject to fingerprinting under this section with the right to complete, correct, and explain information contained in the criminal history records prior to any final adverse determination.

d. (1) The Commission may establish and collect fees to process fingerprints and criminal history records under this section.

(2) Notwithstanding section 3302(b) of title 31, United States Code, and to the extent approved in appropriation Acts—

(A) a portion of the amounts collected under this subsection in any fiscal year may be retained and used by the Commission to carry out this section; and

(B) the remaining portion of the amounts collected under this subsection in such fiscal year may be transferred periodically to the Attorney General and used by the Attorney General to carry this section.

(3) Any amount made available for use under paragraph (2) shall remain available until expended.

* * * * * * *

CHAPTER 18. ENFORCEMENT

SEC. 221. [42 U.S.C. 2271] GENERAL PROVISIONS.—

a. To protect against the unlawful dissemination of Restricted Data and to safeguard facilities, equipment, materials, and other property of the Commission, the President shall have authority to utilize the services of any Government agency to the extent he may deem necessary or desirable.

b. The Federal Bureau of Investigation of the Department of Justice shall investigate all alleged or suspected criminal violations of this Act.

c. No action shall be brought against any individual or person for any violation under this Act unless and until the Attorney General of the United States has advised the Commission with respect to such action and no such action shall be commenced except by the Attorney General of the United States: *Provided, however,* That no action shall be brought under section 222, 223, 224, 225 or 226 except by the express direction of the Attorney General: *And provided further,* That nothing in this subsection shall be construed as applying to administrative action taken by the Commission.

SEC. 222. [42 U.S.C. 2272] VIOLATION OF SPECIFIC SECTIONS.—

Whoever willfully violates, attempts to violate, or conspires to violate, any provision of sections 57, 92, or 101, or whoever unlawfully interferes, attempts to interfere, or conspires to interfere with any

recapture or entry under section 108 shall, upon conviction thereof, be punished by a fine of not more than $10,000 or by imprisonment for not more than ten years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation shall, upon conviction thereof, be punished by imprisonment for life, or by imprisonment for any terms of years or a fine of not more than $20,000 or both.

SEC. 223. [42 U.S.C. 2273] VIOLATION OF SECTIONS GENERALLY.—

a. Whoever willfully violates, attempts to violate, or conspires to violate, any provision of this Act for which no criminal penalty is specifically provided or of any regulation or order prescribed or issued under section 65 or subsections 161 b., i., or o. shall, upon conviction thereof, be punished by a fine of not more than $5,000 or by imprisonment for not more than two years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation, shall, upon conviction thereof, be punished by a fine of not more than $20,000 or by imprisonment for not more than twenty years, or both.

b. Any individual director, officer, or employee of a firm constructing, or supplying the components of any utilization facility required to be licensed under section 103 or 104 b. of this Act who by act or omission, in connection with such construction or supply, knowingly and willfully violates or causes to be violated, any section of this Act, any rule, regulation, or order issued thereunder, or any license condition, which violation results, or if undetected could have resulted, in a significant impairment of a basic component of such a facility shall, upon conviction, be subject to a fine of not more than $25,000 for each day of violation, or to imprisonment not to exceed two years, or both. If the conviction is for a violation committed after a first conviction under this subsection, punishment shall be a fine of not more than $50,000 per day of violation, or imprisonment for not more than two years, or both. For the purposes of this subsection, the term "basic component" means a facility structure, system, component or part thereof necessary to assure—

(1) the integrity of the reactor coolant pressure boundary,

(2) the capability to shut-down the facility and maintain it in a safe shut-down condition, or

(3) the capability to prevent or mitigate the consequences of accidents which could result in an unplanned offsite release of quantities of fission products in excess of the limits established by the Commission.

The provisions of this subsection shall be prominently posted at each site where a utilization facility required to be licensed under section 103 or 104 b. of this Act is under construction and on the premises of each plant where components for such a facility are fabricated.

SEC. 224. [42 U.S.C. 2274] COMMUNICATION OF RESTRICTED DATA.—Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data—

a. Communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction thereof, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both;

b. communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both.

SEC. 225. [42 U.S.C. 2275] RECEIPT OF RESTRICTED DATA.—Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, acquires or attempts or conspires to acquire any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data shall, upon conviction thereof, be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both.

SEC. 226. [42 U.S.C. 2276] TAMPERING WITH RESTRICTED DATA.—Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, removes, conceals, tampers with, alters, mutilates, or destroys any document, writing, sketch, photograph, plan, model, instrument, appliance, or note involving or incorporating Restricted Data and used by any individual or person in connection with the production of special nuclear material, or research or development relating to atomic energy, conducted by the United States, or financed in whole or in part by Federal funds, or conducted with the aid of special nuclear material, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both.

SEC. 227. [42 U.S.C. 2277] DISCLOSURE OF RESTRICTED DATA.—Whoever, being or having been an employee or member of the Commission, a member of the Armed Forces, an employee of any agency of the United States, or being or having been a contractor of the Commission or of an agency of the United States, or being or having been an employee of a contractor of the Commission or of an agency of the United States, or being or having been a licensee of the Commission, or being or having been an employee of a licensee of the Commission, knowingly communicates, or whoever conspires to communicate or to receive, any Restricted Data, knowing or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data pursuant to the provisions of this Act or under rule or regulation of the Commission issued pursuant thereto, knowing or having reason to believe such person is not so authorized to receive Restricted Data shall, upon conviction thereof, be punishable by a fine of not more than $2,500.

SEC. 228. [42 U.S.C. 2278] STATUTE OF LIMITATIONS.—Except for a capital offense, no individual or person shall be prosecuted, tried, or punished for any offense prescribed or defined in sections 224 to 226, inclusive, of this Act, unless the indictment is found or the information is instituted within ten years next after such offense shall have been committed.

SEC. 229. [42 U.S.C. 2278a] TRESPASS UPON COMMISSION INSTALLATIONS.—

a. The Commission is authorized to issue regulations relating to the entry upon or carrying, transporting or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Commission. Every such regulation of the Commission shall be posted conspicuously at the location involved.

b. Whoever shall willfully violate any regulation of the Commission issued pursuant to subsection a. shall, upon conviction thereof, be punishable by a fine of not more than $1,000.

c. Whoever shall willfully violate any regulation of the Commission issued pursuant to subsection a. with respect to any installation or other property which is enclosed by a fence, wall, floor, roof, or other structural barrier shall be guilty of a misdemeanor and upon conviction thereof shall be punished by a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

SEC. 230. [42 U.S.C. 2278b] PHOTOGRAPHING, ETC., OF COMMISSION INSTALLATIONS.—It shall be an offense, punishable by a fine of not more than $1,000 or imprisonment for not more than one year, or both—

(1) to make any photograph, sketch, picture, drawing, map or graphical representation, while present on property subject to the jurisdiction, administration or in the custody of the Commission, of any installations or equipment designated by the President as requiring protection against the general dissemination of information relative thereto, in the interest of the common defense and security, without first obtaining the permission of the Commission, and promptly submitting the product obtained to the Commission for inspection or such other action as may be deemed necessary; or

(2) to use or permit the use of an aircraft or any contrivance used, or designed for navigation or flight in air, for the purpose of making a photograph, sketch, picture, drawing, map or graphical representation of any installation or equipment designated by the President as provided in the preceding paragraph, unless authorized by the Commission.

SEC. 231. [42 U.S.C. 2279] OTHER LAWS.—Sections 224 to 230 shall not exclude the applicable provisions of any other laws.

SEC. 232. [42 U.S.C. 2280] INJUNCTION PROCEEDINGS.—Whenever in the judgment of the Commission any person has engaged or is about to engage in any acts or practices which constitute or will constitute a violation of any provision of this Act, or any regulation

or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with such provision, and upon a showing by the Commission that such person has engaged or is about to engage in any such acts or practices a permanent or temporary injunction, restraining order, or other order may be granted.

SEC. 233. [42 U.S.C. 2281] CONTEMPT PROCEEDINGS.—In case of failure or refusal to obey a subpena served upon any person pursuant to subsection 161 c., the district court for any district in which such person is found or resides or transacts business, upon application by the Attorney General on behalf of the United States, shall have jurisdiction to issue an order requiring such person to appear and give testimony or to appear and produce documents, or both, in accordance with the subpena; and any failure to obey such order of the court may be punished by such court as a contempt thereof.

SEC. 234. [42 U.S.C. 2282] CIVIL MONETARY PENALTIES FOR VIOLATIONS OF LICENSING REQUIREMENTS.—

a. Any person who (1) violates any licensing provision of section 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 or any rule, regulation, or order issued thereunder, or any term, condition, or limitation of any license issued thereunder, or (2) commits any violation for which a license may be revoked under section 186, shall be subject to a civil penalty, to be imposed by the Commission, of not to exceed $100,000 for each such violation. If any violation is a continuing one, each day of such violation shall constitute a separate violation for the purpose of computing the applicable civil penalty. The Commission shall have the power to compromise, mitigate, or remit such penalties.

b. Whenever the Commission has reason to believe that a person has become subject to the imposition of a civil penalty under the provisions of this section, it shall notify such person in writing (1) setting forth the date, facts, and nature of each act or omission with which the person is charged, (2) specifically identifying the particular provision or provisions of the section, rule, regulation, order, or license involved in the violation, and (3) advising of each penalty which the Commission proposes to impose and its amount. Such written notice shall be sent by registered or certified mail by the Commission to the last known address of such person. The person so notified shall be granted an opportunity to show in writing, within such reasonable period as the Commission shall by regulation prescribe, why such penalty should not be imposed. The notice shall also advise such person that upon failure to pay the civil penalty subsequently determined by the Commission, if any, the penalty may be collected by civil action.

c. On the request of the Commission, the Attorney General is authorized to institute a civil action to collect a penalty imposed pursuant to this section. The Attorney General shall have the exclusive power to compromise, mitigate, or remit such civil penalties as are referred to him for collection.

SEC. 235. [42 U.S.C. 2283] PROTECTION OF NUCLEAR INSPECTORS.—

a. Whoever kills any person who performs any inspections which—

(1) are related to any activity or facility licensed by the Commission, and

(2) are carried out to satisfy requirements under this Act or under any other Federal law governing the safety of utilization facilities required to be licensed under section 103 or 104 b., or the safety of radioactive materials

shall be punished as provided under sections 1111 and 1112 of title 18, United States Code. The preceding sentence shall be applicable only if such person is killed while engaged in the performance of such inspection duties or on account of the performance of such duties.

b. Whoever forcibly assaults, resists, opposes, impedes, intimidates, or interferes with any person who performs inspections as described under subsection a. of this section, while such person is engaged in such inspection duties or on account of the performance of such duties, shall be punished as provided under section 111 of title 18, United States Code.

SEC. 236. [42 U.S.C. 2284] SABOTAGE OF NUCLEAR FACILITIES OR FUEL.—Any person who intentionally and willfully destroys or causes physical damage to, or who intentionally and willfully attempts to destroy or cause physical damage to—

(1) any production facility or utilization facility licensed under this Act,

(2) any nuclear waste storage facility licensed under this Act,

(3) any nuclear fuel for such a utilization facility, or any spent nuclear fuel from such a facility,

shall be fined not more than $10,000 or imprisoned for not more than ten years, or both.

SECTION 705 OF THE COMMUNICATIONS ACT OF 1934 (47 U.S.C. 605) (UNAUTHORIZED PUBLICATION OF COMMUNICATIONS)

UNAUTHORIZED PUBLICATION OF COMMUNICATIONS

SEC. 705. (a) Except as authorized by chapter 119, title 18, United States Code, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communica-

APPENDIX C

Executive Order 12356

APPENDIX D

Selected DoD Issuances

Department of Defense
DIRECTIVE

November 15, 1991
NUMBER 5210.83

ASD(C3I)

SUBJECT: Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)

References:
(a) Section 128 of title 10, United States Code
(b) DoD 5400.7-R, "DoD Freedom of Information Act Program," October 1990, authorized by DoD Directive 5400.7, May 13, 1988
(c) Section 552 of title 5, United States Code
(d) CG-W-5, "Joint DOE/DoD Nuclear Weapon Classification Policy Guide," the Department of Energy and the Department of Defense, January 1984
(e) through (k), see enclosure 1

A. PURPOSE

This Directive implements reference (a) by establishing policy, assigning responsibilities, and prescribing procedures for identifying, controlling, and limiting the dissemination of unclassified information on the physical protection of DoD special nuclear material (SNM), equipment, and facilities. That information shall be referred to as "the Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)," to distinguish it from a similar Department of Energy (DoE) program.

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2. Implements reference (a), which is the statutory basis for controlling the DoD UCNI in the Department of Defense. Reference (a) also constitutes the authority for invoking reference (b) to prohibit mandatory disclosure of DoD UCNI under the "Freedom of Information Act (FOIA)" in reference (c).

3. Supplements the security classification guidance contained in reference (d) and CG-SS-1 and DoD Instruction 5210.67 (references (e) and (f)) by establishing procedures for

identifying, controlling, and limiting the dissemination of unclassified information on the physical protection of DoD SNM.

4. Applies to all SNM, regardless of form, in reactor cores or to other items under the direct control of the DoD Components.

5. Applies equally to DoE UCNI under DoD control, except the statute applicable to DoE UCNI (42 U.S.C. 2011 et seq., reference (g)) must be used with the concurrence of the DoE as the basis for invoking the FOIA (Section 552 of 10 U.S.C., reference (c)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD policy:

1. To prohibit the unauthorized dissemination of unclassified information on security measures, including security plans, procedures, and equipment for the physical protection of DoD SNM, equipment, or facilities.

2. That the decision to protect unclassified information as DoD UCNI shall be based on a determination that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

3. That government information shall be made publicly available to the fullest extent possible by applying the minimum restrictions consistent with the requirements of 10 U.S.C. 128 (reference (a)) necessary to protect the health and safety of the public or the common defense and security.

4. That nothing in this Directive prevents a determination that information previously determined to be DoD UCNI is classified information under applicable standards of classification.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

a. Administer the DoD program for controlling DoD UCNI.

b. Coordinate DoD compliance with the DoE program for controlling DoE UCNI.

c. Prepare and maintain the reports required by 10 U.S.C. 128 (reference (a)).

2. The Assistant Secretary of Defense (Public Affairs) shall provide guidance to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)), other elements of the OSD, and the Heads of the DoD Components on the FOIA (5 U.S.C. 552, reference (c)), as implemented in DoD 5400.7-R (reference (b)), as it applies to the DoD UCNI Program.

3. The Heads of the DoD Components shall:

a. Implement this Directive in their DoD Components.

b. Advise the ASD(C3I) of the following, when information not in the guidelines in enclosure 4 is determined to be DoD UCNI:

(1) Identification of the type of information to be controlled as DoD UCNI. It is not necessary to report each document or numbers of documents.

(2) Justification for identifying the type of information as DoD UCNI, based on the guidelines in enclosure 4 and prudent application of the adverse effects test.

F. PROCEDURES

Enclosure 3 outlines the procedures for controlling DoD UCNI. Enclosure 4 provides general and topical guidelines for identifying information that may qualify for protection as DoD UCNI. The procedures and guidelines in enclosures 3 and 4 complement the DoD Component programs to protect other DoD-sensitive unclassified information and may be used with them.

G. INFORMATION REQUIREMENTS

1. Section 128 of 10 U.S.C. (reference (a)) requires that the Secretary of Defense prepare on a quarterly basis a report to be made available on the request of any interested person. Enclosure 3 outlines the procedures for preparing the quarterly report.

2. The report is exempt from licensing in accordance with DoD 7750.5-M, paragraph E.4.e. (reference (h)).

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Assistant Secretary of Defense

for Command, Control, Communications, and Intelligence within 120 days; forward one copy of changes to implementing documents within 90 days of publication.

Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 4
1. References
2. Definitions
3. Procedures for Identifying and Controlling DoD UCNI
4. Guidelines for the Determination of DoD UCNI

REFERENCES, continued

(e) CG-SS-1, "Safeguards and Security Classification Guide," the Department of Energy, September 1985
(f) DoD Instruction 5210.67, "Special Nuclear Material Information, Security Classification Guidance," December 3, 1982
(g) Section 2011 *et seq.* of title 42, United States Code
(h) DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986
(i) DoE GG-2, "Department of Energy Unclassified Controlled Nuclear Information General Guidelines," the Department of Energy, August 1989
(j) Department of Energy Order 5635.4, "Protection of Unclassified Controlled Nuclear Information," February 3, 1988
(k) Department of Energy Order 5650.3, "Identification of Unclassified Controlled Nuclear Information," February 29, 1988

DEFINITIONS

1. Atomic Energy Defense Programs. Activities, equipment, and facilities of the Department of Defense used or engaged in support of the following:

a. Development, production, testing, sampling, maintenance, repair, modification, assembly, utilization, transportation, or retirement of nuclear weapons or nuclear weapon components.

b. Production, utilization, or transportation of DoD SNM for military applications.

c. Safeguarding of activities, equipment, or facilities that support the functions in definitions 1.a. and 1.b., above, including the protection of nuclear weapons, nuclear weapon components, or DoD SNM for military applications at a fixed facility or in transit.

2. Authorized Individual. A person who has been granted routine access to specific DoD UCNI under 10 U.S.C. 128 (reference (a)).

3. Denying Official. An individual who denies a request made under 5 U.S.C. 552 for all, or any portion, of a document or material containing DoD UCNI.

4. Document or Material. The physical medium on, or in, which information is recorded, or a product or substance which contains or reveals information, regardless or its physical form or characteristics.

5. Information. Any fact or concept regardless of the physical form or characteristics of the medium on, or in, which it is recorded, contained or revealed.

6. Reviewing Official. An individual who may make a determination that a document or material contains, does not contain, or no longer contains DoD UCNI.

7. Safeguards. An integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of DoD SNM, equipment or facilities.

8. Special Nuclear Material Facility. A DoD facility that performs a sensitive function (see definition 9., below).

9. Sensitive Function. A function in support of atomic energy defense programs whose disruption could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security (see definition 1., above).

10. Special Nuclear Material (SNM). Plutonium, uranium enriched in the isotope-233 or in the isotope-235, except source material or any material artificially enriched by any of the foregoing.

11. Special Nuclear Material Equipment. Equipment, systems, or components whose failure or destruction would cause an impact on safeguarding DoD SNM resulting in an unacceptable interruption to a national security program or an unacceptable impact on the health and safety of the public.

12. Unauthorized Dissemination. The intentional or negligent transfer, in any manner and by any person, of information contained in a document or material determined by a reviewing official to contain DoD UCNI, and so marked in accordance with the procedures in Enclosure 3, to any person or entity other than an authorized individual or a person granted special access to specific DoD UCNI under 10 U.S.C. 128 (reference (a)).

PROCEDURES FOR IDENTIFYING AND CONTROLLING DoD UCNI

A. GENERAL

1. The Secretary of Defense's authority for prohibiting the unauthorized disclosure and dissemination of DoD UCNI may be exercised by the Heads of the DoD Components and by the officials to whom such authority is specifically delegated by the Heads of the DoD Components. These procedures for identifying and controlling DoD UCNI are provided as guidance for the Heads of the DoD Components to implement the Secretary of Defense's authority to prohibit the unauthorized dissemination of unclassified information on security measures, including security plans, procedures, and equipment, for the physical protection of DoD SNM, equipment, or facilities.

2. The decision to protect unclassified information as DoD UCNI shall be based on a determination that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

3. Government information shall be made publicly available to the fullest extent possible by applying the minimum restrictions consistent with the requirements of 10 U.S.C. 128 (reference (a)) necessary to protect the health and safety of the public or the common defense and security.

4. DoD personnel, in making a determination to protect unclassified information as DoD UCNI, shall consider the probability of an illegal production, theft, diversion, or sabotage if the information proposed for protection were made available for public disclosure and dissemination. The determination to protect specific documents or information is not related to the ability of DoD UCNI to be obtained by other sources. For determining the control of DoD UCNI, the cognizant official should consider how the unauthorized disclosure or dissemination of such information could assist a potential adversary in the following:

a. Selecting a target for an act of theft, diversion, or sabotage of DoD SNM, equipment, or facilities (e.g., relative importance of a facility or the location, form, and quantity of DoD SNM). Information that can be obtained by observation from public areas outside controlled locations should not be considered as DoD UCNI.

b. Planning or committing an act of theft, diversion, or sabotage of DoD SNM, equipment, or facilities (e.g., design of security systems; building plans; methods and procedures for

transfer, accountability, and handling of DoD SNM; or security plans, procedures, and capabilities).

c. Measuring the success of an act of theft, diversion, or sabotage of DoD SNM, equipment, or facilities (e.g., actual or hypothetical consequences of the sabotage of specific vital equipment or facilities).

d. Illegally producing a nuclear explosive device (e.g., unclassified nuclear weapon design information useful in designing a primitive nuclear device; location of unique DoD SNM needed to fabricate such a device; or location of a nuclear weapon).

e. Dispersing DoD SNM in the environment (e.g., location, form, and quantity of DoD SNM).

5. DoD UCNI shall be identified, controlled, marked, transmitted, and safeguarded in the DoD Components, the North Atlantic Treaty Organization (NATO), and among DoD contractors, consultants, and grantees authorized to conduct official business for the Department of Defense. Contracts requiring the preparation of unclassified information that could be DoD UCNI shall have the requirements for identifying and controlling the DoD UCNI.

6. DoE GG-2 and DoE Orders 5635.4 and 5650.3 (references (i), (j), and (k)) provide background on implementation of the UCNI Program in the DoE. The DoD Components maintaining custody of DoE UCNI should refer to those documents for its identification and control.

B. IDENTIFYING DoD UCNI

1. To be considered for protection as DoD UCNI, the information must:

a. Be unclassified.

b. Pertain to security measures, including plans, procedures, and equipment, for the physical protection of DoD SNM, equipment, or facilities.

c. Meet the adverse effects test; i.e., that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

2. Information, in the categories in section C. of enclosure 4, about DoD SNM should be considered for protection as DoD UCNI.

3. Material originated before the effective date of those procedures, which is found in the normal course of business to have DoD UCNI, shall be protected as DoD UCNI. There is no requirement to conduct detailed file searches to retroactively identify and control DoD UCNI. As existing documents or materials are withdrawn from file, they should be reviewed to determine if they meet the criteria for protection as DoD UCNI and marked and controlled, accordingly.

C. ACCESS TO DOD UCNI.

1. A Reviewing Official is an Authorized Individual for documents or materials that the Reviewing Official determines to contain DoD UCNI. An Authorized Individual, for DoD UCNI, may determine that another person is an Authorized Individual who may be granted routine access to the DoD UCNI, and who may further disseminate the DoD UCNI under the procedures specified in paragraph E., below. This recipient of DoD UCNI from an Authorized Individual is also an Authorized Individual for the specific DoD UCNI to which routine access has been granted. An Authorized Individual designates another person to be an Authorized Individual by the act of giving that person a document or material that contains DoD UCNI. No explicit designation or security clearance is required. This second Authorized Individual may further disseminate the UCNI under the procedures specified in paragraph E., below.

2. A person granted routine access to DoD UCNI must have a need to know the specific DoD UCNI in the performance of official duties or of DoD-authorized activities. The recipient of the document or material shall be informed of the physical protection and access requirements for DoD UCNI. In addition to a need to know, the person must meet at least one of the following requirements:

a. The person is a U.S. citizen who is one of the following:

(1) A Federal Government employee or member of the U.S. Armed Forces;

(2) An employee of a Federal Government contractor, subcontractor, or of a prospective Federal Government contractor or subcontractor who will use the DoD UCNI for the purpose of bidding on a Federal Government contract or subcontract;

(3) A Federal Government consultant or DoD advisory committee member;

(4) A member of Congress;

(5) A staff member of a congressional committee or of an individual Member of Congress;

(6) The Governor of a State or designated State government official or representative;

(7) A local government official or an Indian tribal government official; or

(8) A member of a State, local, or Indian tribal law enforcement or emergency response organization.

b. The person is other than a U.S. citizen, and is one of the following:

(1) A Federal Government employee or a member of the U.S. Armed Forces;

(2) An employee of a Federal Government contractor or subcontractor; or

(3) A Federal Government consultant or DoD advisory committee member.

c. The person may be other than a U.S. citizen who is not otherwise eligible for routine access to DoD UCNI under paragraph 2.b., above, but who requires routine access to specific DoD UCNI in conjunction with one of the following:

(1) An international nuclear cooperative activity approved by the Federal Government;

(2) U.S. diplomatic dealings with foreign government officials; or

(3) Provisions of treaties, mutual defense acts, or Government contracts or subcontracts.

3. A person not authorized routine access to DoD UCNI under paragraph 2., above, may submit a request for special access to DoD UCNI to Heads of DoD Components, or their designated representative, as appropriate. A special access request must include the following information:

a. The name, current residence or business address, birthplace, birth date, and country of citizenship of the person submitting the request;

b. A description of the DoD UCNI for which special access is being requested;

c. A description of the purpose for which the DoD UCNI is needed; and

d. Certification by the requester of his or her understanding of, and willingness to abide by, the requirements for the protection of DoD UCNI contained in this Directive.

4. Heads of DoD Components, or their designated representative, shall base his or her decision to grant special access to DoD UCNI on an evaluation of the following criteria:

a. The sensitivity of the DoD UCNI for which special access is being requested (i.e., the worst-case, adverse effect on the health and safety of the public or the common defense and security which would result from unauthorized use of the DoD UCNI);

b. The purpose for which the DoD UCNI is needed (e.g., the DoD UCNI will be used for commercial or other private purposes, or will be used for public benefit to fulfill statutory or regulatory responsibilities);

c. The likelihood of an unauthorized dissemination by the requester of the DoD UCNI; and

d. The likelihood of the requester using the DoD UCNI for illegal purposes.

5. Heads of DoD Components, or their designated representative, shall attempt to notify a person who requests special access to DoD UCNI within 30 days of receipt of the request as to whether or not special access to the requested DoD UCNI is granted. If a final determination on the request cannot be made within 30 days of receipt of the request, Heads of DoD Components, or their designated representative, shall notify the requester, within 30 days of the request, as to when the final determination on the request may be made.

6. A person granted special access to specific UCNI is not an Authorized Individual and shall not further disseminate the DoD UCNI to which special access has been granted.

7. An Authorized Individual granting routine access to specific DoD UCNI to another person shall notify each person granted access (other than when the person being granted such access is a Federal Government employee, a member of the U.S. Armed Forces, or an employee of a Federal Government contractor or subcontractor) of applicable regulations concerning the protection of DoD UCNI and of any special dissemination limitations that the Authorized Individual determines to apply for the specific DoD UCNI to which routine access is being granted.

8. Heads of DoD Components, or their designated representative, shall notify each person granted special access to DoD UCNI of applicable regulations concerning the protection of DoD UCNI prior to dissemination of the DoD UCNI to the person.

9. The requirement to notify persons granted routine access or special access to specific DoD UCNI may be met by attachment of an appropriate cover sheet to the front of each document or material containing DoD UCNI prior to its transmittal to the person granted access.

D. MARKINGS

1. An unclassified document with DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the bottom on the outside of the front cover, if any, and on the outside of the back cover, if any.

2. In an unclassified document, an individual page that has DoD UCNI shall be marked to show which of its portions contain DoD UCNI information. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(DoD UCNI)" shall be used and placed at the beginning of those portions with DoD UCNI.

3. In a classified document, an individual page that has both DoD UCNI and classified information shall be marked at the top and bottom of the page with the highest security classification of information appearing on that page. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(DoD UCNI)" shall be used and placed at the beginning of those portions with DoD UCNI. In a classified document, an individual page that has DoD UCNI, but no classified information, shall be marked "DoD Unclassified Controlled Information" at the bottom of the page. The DoD UCNI marking may be combined with other markings, if all relevant statutory and regulatory citations are included.

4. Other material (e.g., photographs, films, tapes, or slides) shall be marked "DoD Unclassified Controlled Nuclear Information" to ensure that a recipient or viewer is aware of the status of the information.

E. DISSEMINATION AND TRANSMISSION

1. DoD UCNI may be disseminated in the DoD Components, the NATO, and among the DoD contractors, consultants, and grantees on a need-to-know basis to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or dissemination. Contracts that shall require access to DoD UCNI shall require compliance with this Directive and the DoD Component regulations and have the requirements for the marking, handling, and safeguarding of DoD UCNI.

2. DoD holders of DoD UCNI are authorized to convey such information to officials in other Departments or Agencies on a need-to-know basis to fulfill a Government function. Transmittal documents shall call attention to the presence of

DoD UCNI attachments using an appropriate statement in the text, or marking at the bottom of the transmittal document, that "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)." Similarly, documents transmitted shall be marked, as prescribed in section D., above.

3. DoD UCNI transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the DoD UCNI marking. That may be accomplished by typing or stamping the following statement on the document before transfer:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE
(5 U.S.C. 552(b)(3), as authorized by 10 U.S.C. 128)

4. When not commingled with classified information, DoD UCNI may be sent by first-class mail in a single, opaque envelope or wrapping.

5. DoD UCNI may only be discussed or transmitted over an unprotected telephone or telecommunications circuit (to include facsimile transmissions) in an emergency.

6. Each part of electronically transmitted messages with DoD UCNI shall be marked appropriately. Unclassified messages with DoD UCNI shall have the abbreviation "DoD UCNI" before the beginning of the text.

7. DoD UCNI may be processed, stored, or produced on stand-alone personal computers, or shared-logic word processing systems, if protection from unauthorized disclosure or dissemination, in accordance with the procedures in section F., below, can be ensured.

8. A document marked as having DoD UCNI may be reproduced minimally without permission of the originator and consistent with the need to carry out official business.

F. <u>SAFEGUARDING DoD UCNI</u>

1. During normal working hours, documents determined to have DoD UCNI shall be placed in an out-of-sight location, or otherwise controlled, if the work area is accessible to unescorted personnel.

2. At the close of business, DoD UCNI material shall be stored so to preclude disclosure. Storage of such material with other unclassified documents in unlocked receptacles; i.e., file cabinets, desks, or bookcases, is adequate, when normal Government or Government-contractor internal building security is provided during nonduty hours. When such internal building security is not provided, locked rooms or buildings normally

provide adequate after-hours protection. If such protection is not considered adequate, DoD UCNI material shall be stored in locked receptacles; i.e., file cabinets, desks, or bookcases.

3. Nonrecord copies of DoD UCNI materials must be destroyed by tearing each copy into pieces to reasonably preclude reconstruction and placing the pieces in regular trash containers. If the sensitivity or volume of the information justifies it, DoD UCNI material may be destroyed in the same manner as classified material rather than by tearing. Record copies of DoD UCNI documents shall be disposed of, in accordance with the DoD Components' record management regulations. DoD UCNI on magnetic storage media shall be disposed of by overwriting to preclude its reconstruction.

4. The unauthorized disclosure of DoD UCNI material does not constitute disclosure of DoD information that is classified for security purposes. Such disclosure of DoD UCNI justifies investigative and administrative actions to determine cause, assess impact, and fix responsibility. The DoD Component that originated the DoD UCNI information shall be informed of its unauthorized disclosure and the outcome of the investigative and administrative actions.

G. RETIREMENT OF DOCUMENT OR MATERIAL

1. Any unclassified document or material which is not marked as containing DoD UCNI but which may contain DoD UCNI shall be marked upon retirement in accordance with the DoD Components' record management regulations.

2. A document or material marked as containing DoD UCNI is not required to be reviewed by a Reviewing Official upon or subsequent to retirement. A Reviewing Official shall review any retired document or material upon a request for its release made under 5 U.S.C. 552 (reference (c))

H. REQUESTS FOR PUBLIC RELEASE OF DoD UCNI

DoD 5400.7-R (reference (b)) applies. Information that qualifies as DoD UCNI, under 10 U.S.C. 128 (reference (a)), is exempt from mandatory disclosure under 5 U.S.C. 552 (reference (c)). Consequently, requests for the public release of DoD UCNI shall be denied under Section 552(b)(3) of reference (c), citing reference (a) as authority.

I. REPORTS

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall prepare and maintain the quarterly reports required by 10 U.S.C. 128 (reference (a)). The Heads of the DoD Components shall advise the ASD(C3I) when information not in the guidelines in enclosure

4 is determined to be DoD UCNI. Those reports shall have the following information:

(1) Identification of the information to be controlled as DoD UCNI. It is not necessary to report each document or numbers of documents.

(2) Justification for identifying the type of information to be controlled as DoD UCNI.

(3) Certification that only the minimal information necessary to protect the health and safety of the public or the common defense and security is being controlled as DoD UCNI.

GUIDELINES FOR THE DETERMINATION OF DoD UCNI

A. USE OF DETERMINATION OF DoD UCNI GUIDELINES

1. These guidelines for determining DoD UCNI are the bases for determining what unclassified information about the physical protection of DoD SNM, equipment, or facilities in a given technical or programmatic subject area is DoD UCNI.

2. The decision to protect unclassified information as DoD UCNI shall be based on a determination that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of SNM, equipment, or facilities.

B. GENERAL

1. The policy for protecting unclassified information about the physical protection of DoD SNM, equipment, or facilities is to protect the public's interest by controlling certain unclassified Government information so to prevent the adverse effects described in section D. of this Directive and in enclosure 3, without restricting public availability of information that would not result in those adverse effects.

2. In controlling DoD SNM information, only the minimum restrictions needed to protect the health and safety of the public or the common defense and security shall be applied to prohibit the disclosure and dissemination of DoD UCNI.

3. Any material that has been, or is, widely and irretrievably disseminated into the public domain and whose dissemination was not, or is not, under Government control is exempt from control under these guidelines. However, the fact that information is in the public domain is not a sufficient basis for determining that similar or updated Government-owned and -controlled information in another document or material is not, or is no longer, DoD UCNI; case-by-case determinations are required.

C. TOPICAL GUIDANCE

The following elements of information shall be considered by the DoD Components during the preparation of unclassified information about the physical protection of DoD SNM to determine if it qualifies for control as DoD UCNI:

1. Vulnerability Assessments

a. General vulnerabilities that could be associated with specific DoD SNM, equipment, or facility locations.

b. The fact that DoD SNM facility security-related projects or upgrades are planned or in progress.

c. Identification and description of security system components intended to mitigate the consequences of an accident or act of sabotage at a DoD SNM facility.

2. Material Control and Accountability

a. Total quantity or categories of DoD SNM at a facility.

b. Control and accountability plans or procedures.

c. Receipts that, cumulatively, would reveal quantities and categories of DoD SNM of potential interest to an adversary.

d. Measured discards, decay losses, or losses due to fission and transmutation for a reporting period.

e. Frequency and schedule of DoD SNM inventories.

3. Facility Description

a. Maps, conceptual design, and construction drawings of a DoD SNM facility showing construction characteristics of building and associated electrical systems, barriers, and back-up power systems not observable from a public area.

b. Maps, plans, photographs, or drawings of man-made or natural features in a DoD SNM facility not observable from a public area: i.e., tunnels, storm or waste sewers, water intake and discharge conduits, or other features having the potential for concealing surreptitious movement.

4. Intrusion Detection and Security Alarm Systems

a. Information on the layout or design of security and alarm systems at a specific DoD SNM facility, if the information is not observable from a public area.

b. The fact that a particular system make or model has been installed at a specific DoD SNM facility, if the information is not observable from a public area.

c. Performance characteristics of installed systems.

5. Keys, Locks, Combinations, and Tamper-Indicating Devices

a. Types and models of keys, locks, and combinations of locks used in DoD SNM facilities and during shipment.

b. Method of application of tamper-indicating devices.

c. Vulnerability information available from unclassified vendor specifications.

6. Threat Response Capability and Procedures

a. Information about arrangements with local, State, and Federal law enforcement Agencies of potential interest to an adversary.

b. Information in "nonhostile" contingency plans of potential value to an adversary to defeat a security measure; i.e., fire, safety, nuclear accident, radiological release, or other administrative plans.

c. Required response time of security forces.

7. Physical Security Evaluations

a. Method of evaluating physical security measures not observable from public areas.

b. Procedures for inspecting and testing communications and security systems.

8. In-Transit Security

a. Fact that a shipment is going to take place.

b. Specific means of protecting shipments.

c. Number and size of packages.

d. Mobile operating and communications procedures that could be exploited by an adversary.

e. Information on mode, routing, protection, communications, and operations that must be shared with law enforcement or other civil agencies, but not visible to the public.

f. Description and specifications of transport vehicle compartments or security systems not visible to the public.

9. Information on Nuclear Weapon Stockpile and Storage Requirements, Nuclear Weapon Destruction and Disablement Systems, and Nuclear Weapon Physical Characteristics. Refer to CG-W-5 (reference (d)) for guidance about the physical

protection of information on nuclear weapon stockpile and storage requirements, nuclear weapon destruction and disablement systems, and nuclear weapon physical characteristics that may, under certain circumstances, be unclassified. Such information meeting the adverse effects test shall be protected as DoD UCNI.