# WHITE PAPER
# CLASSIFICATION AND DECLASSIFICATION WITHIN THE DEPARTMENT OF DEFENSE

## INSPECTOR GENERAL
## DEPARTMENT OF DEFENSE

MAY 1995

## ACRONYMS

| | |
|---|---|
| **ASD(C3I)** | Assistant Secretary of Defense (Command, Control, Communications and Intelligence) |
| **DASD(CI&SCM)** | Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures |
| **DASD(I&S)** | Deputy Assistant Secretary of Defense for Intelligence and Security |
| **DMA** | Defense Mapping Agency |
| **GAO** | General Accounting Office |
| **ISOO** | Information Security Oversight Office |
| **NARA** | National Archives and Records Administration |
| **OADR** | Originating Agency's Determination Required |
| **OCA** | Original Classification Authority |
| **SAP** | Special Access Program |
| **SCI** | Sensitive Compartmented Information |
| **SF** | Standard Form |

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

MAY 24 1995

MEMORANDUM FOR DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY

SUBJECT: Classification and Declassification within the Department of Defense

Enclosed is a white paper addressing the policies and procedures governing the classification and declassification processes established within the Department of Defense. This paper was originally requested by the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures before the office was merged into yours. It is intended to assist you in addressing classification and declassification issues throughout the Department of Defense (DoD).

In this paper, we reviewed the policy guidance related to each component of the classification-declassification system and examined how that policy is implemented in practice by selected DoD activities within the National Capital Region. Our effort concludes that the classification process is fundamentally sound, understood and implemented within DoD, but that elements of the declassification process are ineffective. The declassification process is overshadowed by the continuing emphasis on classification and the protection of information. Efforts to improve the classification-declassification system should focus on the declassification process. We provide specific suggestions to improve the declassification process by focusing on a risk management philosophy and related procedures to accomplish declassification as a matter of routine.

The goal of the Program Evaluation Directorate is to study and assess various programs, activities and processes within the DoD to provide information and insights that Defense offices and organizations need but may not have the internal resources to pursue on their own. As a result, the suggestions offered in this paper are discretionary and there is no formal Inspector General follow-up action.

We hope this report will be of value to you. Your feedback would be appreciated. Should you need additional information, or if you have additional areas in which you need assistance, please call Mr. Frank Griggs, Project Director, at (703) 604-8755.

John C. Speedy, III
Deputy Assistant Inspector General
for Program Evaluation

Enclosure

# EXECUTIVE SUMMARY

We prepared this paper at the request of the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures, since merged into the Deputy Secretary of Defense for Intelligence and Security. The initial purpose of our effort was to assess the policy and procedures of one aspect of the DoD Information Security Program, the classification-declassification system, and determine the adequacy of its three components: the classification process, the declassification process, and the oversight mechanisms associated with them. However, as a result of our 64 interviews, we narrowed our objectives to two: an assessment of the efficiency and effectiveness of the declassification process, and an assessment of required Information Security Program statistical reporting. Specifically excluded from our evaluation were Sensitive Compartmented Information, Special Access Programs and Information Security Systems.

We first reviewed Executive Order 12346, "National Security Information," April 2, 1982, and past and proposed Executive Orders addressing National Security Information. We then reviewed past and current national, departmental and component policy and procedural guidance. Next, we reviewed a recent General Accounting Office audit of classified information and the report of the Joint Security Commission. Then, we analyzed the Department of Defense Program Data Report for Fiscal Year 1993 and based on reported Information Security Program activity, selected 19 DoD activities to include in this evaluation. Subsequently, we interviewed 64 Information Security Program managers and participants located in 19 Department of Defense activities within the National Capital Region to validate the uniformity of the declassification process. Finally, we employed graphic modeling to illustrate and analyze the operation of the classification-declassification processes.

We conclude that the present size of classified holdings is not the result of too much information being classified without reasonable justification. Rather, it is the result of too much information remaining classified for an extended time. Information remains classified longer than necessary because the Information Security Program puts little emphasis on declassification and the efforts made to declassify information are inadequate. Specifically, our research suggests that:

- The classification process functions essentially as intended.
- The declassification process suffers from deficiencies that seriously impair its operation.
- The oversight mechanisms associated with the system, generally function as intended, except for required annual statistical reporting process which lacks sufficient guidance.

We also believe that Information Security Program managers and participants lost sight of the fact that the purpose of the program is twofold. The first purpose is to satisfy the right of the public to know. The second purpose is to safeguard information from unauthorized disclosure for national security reasons. Without question, there will always be a compelling need to protect certain information for national security reasons. Now that the Cold War is over, however, we suggest that a more even balance can be achieved between the need to protect classified information and the needs of an informed public by reducing the length of time information remains classified. To achieve a better balance between the two purposes of the Information Security Program, we offer the following suggestions for consideration by the Deputy Assistant Secretary of Defense for Intelligence and Security:

- Expand Department of Defense 5200.1-R to include a definition of "permanently valuable Department of Defense records," establish a requirement for Original Classification Authorities to specify a particular "Office of Record" for each classified document created, and require derivative classifiers to cite the "Office(s) of Record identified in classified source materials when derivatively classifying documents.

- Expand Department of Defense 5200.1-R to include both adequate guidance and a readily identifiable, clearly defined methodology for declassification decision-making similar to the prototype methodology illustrated on page 18.

- Adopt risk management as the operating philosophy underlying the Information Security Program and include a discussion of the risk management concept in Department of Defense Directive 5200.1, "DoD Information Security Program," June 7, 1982, and the principles of risk management in Department of Defense 5200.1-R. Ensure that all Information Security Program instruction conducted throughout the Department of Defense reflects the risk management philosophy.

- Direct the Department of Defense Security Institute to develop specific, well-defined reporting criteria for each of the Standard Form 311 data entries and revise the Department of Defense 5200.1-R, "Information Security Program Regulation," June 1, 1986, guidance on the annual reporting of Information Security Program data to include those criteria and designate one common sampling technique for all Department of Defense activities.

Many of the recent proposals to reduce the volume of classified information have concentrated on the review and declassification of information in the National Archives. That is a necessary and worthwhile effort, but it does not represent a long-term solution to the problem. In the long term, the problem must be attacked at the working level, not just in the archives. That means declassification must become just as much of a routine, day-to-day practice among Information Security Program participants as classification is today. The goal must be to reduce the volume of classified information before it arrives in the archives, not after. We believe that the Department of Defense can take the lead in implementing that long-term solution by reorienting the Information Security Program to accord greater emphasis to the needs of the informed public and by taking the actions suggested above.

# TABLE OF CONTENTS

# PART I - INTRODUCTION

**PURPOSE**

This paper was requested by the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures (DASD(CI&SCM))[1] within the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)). The DASD(CI&SCM) was concerned about the large volume of classified information accumulated in files within the Department of Defense (DoD) and asked that we focus on one specific aspect of the DoD Information Security Program (hereafter referred to as the Program), the classification-declassification system. Thus, our purpose was to assess the policy and procedures of the classification-declassification system to determine the adequacy of its three elements: the classification process, the declassification process and the oversight mechanisms associated with those processes.

**TERMINOLOGY**

For reference, the following terms and explanations will be used:

**DoD Information Security Policy**

DoD Directive 5200.1, "DoD Information Security Program," states that the policy is "to assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded as well as to facilitate the flow of unclassified information about DoD operations to the public." DoD 5200.1-R, "Information Security Program Regulation," describes that policy as "to make available to the public as much information concerning DoD activities as possible consistent with the need to protect national security."

**The Classification Process**

The classification process identifies information that requires protection from unauthorized disclosure under the provisions of the Program. Information is classified in two ways, by an Original Classification Authority (OCA) or from a prior OCA decision.

*Original Classification and Authorities*

Original classification occurs when an Original Classification Authority makes an initial determination that a specific item or collection of information is classified at a particular level. Original Classification Authorities (OCAs) are incumbents of specifically designated positions; each is authorized to classify information up to a particular level--TOP SECRET, SECRET or CONFIDENTIAL.

*Derivative Classification*

Once an original classification decision is made, subsequent classification actions related to that same information are "derivative." Derivative classification occurs through two similar, but separate methods. Information is derivatively

[1] Functional responsibility for the DoD Information Security Program was transferred to the Deputy Assistant Secretary of Defense for Intelligence and Security (DASD(I&S)) in February 1994.

classified based on a security classification guide or if the information contained in those new products is extracted from materials that have previously been classified.

**The Declassification Process**

The declassification process identifies information that may be given a lesser degree of protection or that no longer requires protection within the Program. OCAs are assigned downgrading and declassification authority comparable to their classification authority, and OCAs making original classification decisions must concurrently provide declassification instructions. Additional declassification authorities may also be designated to act within their specific functional expertise.

*Declassification Authorities*

Original Classification Authorities are specifically identified as declassification authorities. Those officials may further designate "additional officials within the lowest practicable echelons of command and supervision to exercise downgrading and declassification authority over classified information in their functional areas of interest."

**Oversight Mechanisms**

Oversight mechanisms are the tools and techniques that Departmental managers employ to implement Program policies and procedures. We identified four oversight mechanisms that support the DoD Program: management actions, training, challenges to classification decisions, and statistical reporting.

**OADR**

The acronym "OADR" means "Originating Agency's Determination Required." OADR is a declassification marking placed on information at the time it is classified when the Original Classification Authority cannot determine a future time or date for declassification.

**Multiple Sources**

"Multiple Sources" is the classification authority used when a document is derivatively classified from two or more already classified documents, and would appear on a document as "CLASSIFIED BY: Multiple Sources."

**OBJECTIVES**

We originally had three objectives:

- assess the efficiency and effectiveness of each element of the classification-declassification system to determine whether that system achieves the dual policy goals of safeguarding information from unauthorized disclosure for national security reasons and satisfying the right of the public to know;
- evaluate the adequacy of policy guidance issued for the classification-declassification system to identify any weaknesses in that guidance; and
- identify changes needed to improve the operation of the classification-declassification system.

However, results of early interviews consistently indicated that principal weaknesses in the Information Security Program centered on the declassification process and required annual statistical reporting. Therefore, we narrowed the objectives to two:

- an assessment of the efficiency and effectiveness of the declassification process, and
- an assessment of required Program annual statistical reporting.

## METHODOLOGY

To achieve those objectives, we:

- reviewed Executive Order 12356, "National Security Information," April 2, 1982, and past and proposed future Executive Orders addressing National Security Information;
- reviewed current and past national and Departmental policy documents and associated component level directives, regulations, instructions and guidelines (See Appendix A);
- reviewed the May 1993 General Accounting Office (GAO) Report, "CLASSIFIED INFORMATION--Volume Could be Reduced by Changing Retention Policy," GAO/NSIAD-93-127;
- reviewed the February 28, 1994 Joint Security Commission Report, "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence;"
- analyzed the DoD Program Data Report for Fiscal Year 1993, and based on reported Program activity, we visited a total of 19 activities within the Office of the Secretary of Defense, the Joint Staff, each Military Department and eight Defense Agencies (Appendix B); and
- conducted interviews with 64 military and civilian security and policy staff, acquisition, operations and intelligence personnel within those 19 DoD activities to validate the uniformity of the declassification process.

We conducted a detailed content analysis of applicable policy and procedural guidance documents and related studies to establish baseline standards for the classification and declassification processes. Next, we conducted interviews to assess the efficiency and effectiveness of those processes as implemented by selected DoD activities. We then completed a process comparison to identify similarities and differences between the classification and declassification process. Finally, we used graphic modeling to illustrate the operation of the

classification-declassification system. These actions provided the basis for our analytical conclusions and the foundation from which we developed our suggested improvements.

## SCOPE AND LIMITATIONS

We limited the scope of our effort for several reasons.

- First, the classification and declassification processes are driven by policies and procedures that are uniform throughout the Department of Defense.
- Second, at the client's request and as a matter of economy, we limited data collection to the National Capital Region because program policies and procedures are developed, promulgated, managed and monitored by DoD personnel assigned to DoD activities within the NCR.
- Third, we saw no instance where the process was not uniform, therefore saw no need to expand the sample size given the stated objective.
- Fourth, we excluded Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Information Systems Security materials since separate standards have been established for such information.
- Finally, the problem of declassification has sufficiently wide recognition that we did not do a detailed validation of the issue.

Because the classification and declassification processes are driven by policies and procedures that are uniform throughout the DoD, neither our assessment of the policies and procedures affecting the declassification process nor our assessment of required annual Program statistical reporting is affected by these limitations.

## PRIOR COVERAGE

At the request of the Congress, the United States General Accounting Office (GAO) reviewed the classification of national security information. The review, involving elements of the Departments of Defense and State, the General Services Administration, the National Archives and Records Administration, and the Information Security Oversight Office, examined:

- the reasons for the retention of large volumes of documents as classified for long periods of time;
- documents for classification errors;
- reports on government-wide classification and declassification activity; and

- adherence to policies and procedures.

In its Report to Congressional Requestors, "CLASSIFIED INFORMATION: Volume Could be Reduced by Changing Retention Policy," GAO-93-127, May 1993, the GAO found that there were three principal causes for the large volume of classified information:

- government officials exempted most material from the automatic declassification procedures of the previous executive order because they believed the prescribed maximum period was too short;

- declassification is unnecessarily delayed because automatic declassification periods were virtually eliminated by Executive Order 12356;

- unwarranted classification and marking errors occur regularly and documents are not properly marked to reflect which portions of the documents are classified and which are not.

**OVERVIEW**

Unlike the broad GAO review of established policies and procedures, we focus only on the established declassification process and required Program annual statistical reporting. Therefore, the results of the GAO review do not impact on the scope of our effort. Our results are presented in two sections. Section II discusses the classification process. Section III, provides our assessment of the declassification process and required annual Program statistical reporting, followed by our summary and conclusions.

# PART II - BACKGROUND INFORMATION

**THE POLICY**

The policy that establishes the Information Security Program assigns it a dual purpose of ensuring that information warranting protection against unauthorized disclosure for national security reasons is properly protected and providing information about DoD operations to the public. To meet those goals, the classification-declassification system was established. That system is comprised of three components: the classification process, the declassification process, and oversight mechanisms associated with each. The primary intent of the Program is to protect information. Therefore, the Program puts much more emphasis on safeguarding information than it does on determining what information should be protected. That general emphasis on protection, we found, also affects the declassification process. An understanding of the classification process is essential to an understanding of the declassification process.

## THE CLASSIFICATION PROCESS

**PROCESS EMPHASIZES PROTECTION**

The classification process is closely aligned with the primary purpose of the Program, to protect information. Therefore, that process provides easy entry of information into the protected arena. Executive Order 12356 and DoD Directive 5200.1 establish Program policies and procedures, and require the establishment and administration of the Program to ensure compliance with that policy. DoD 5200.1-R provides further policy and all procedural guidance, and stipulates that "It is the policy of the DoD to make available to the public as much information concerning its activities as possible consistent with the need to protect national security." In consonance with that policy, when protection of information against unauthorized disclosure is appropriate, an original decision to classify that information must be made.

**Original Classification Authorities**

The original classification process begins with the designation of specific Original Classification Authorities. Recognizing the potential impact of the original classification process, the Commission on Government Security in 1957 expressed a need to limit the number of officials authorized to classify or to recommend classification. Since then, repeated reductions in the number of Original Classification Authorities have elevated TOP SECRET Original Classification Authority to the most senior executive personnel within each Defense component. Besides the Secretary of Defense and the Secretaries of the Military Departments, TOP SECRET Original Classification Authorities are typically Under or Assistant Secretaries of Defense, and Directors or Deputy Directors of Defense Agencies. SECRET and CONFIDENTIAL Original Classification Authorities are

generally heads of principle staff elements within those Defense components.

*Classification Criteria*

When making an original classification decision, Original Classification Authorities must:

- determine whether information is within a category authorized for classification;
- determine the amount of damage to national security that would occur if the information was disclosed;
- determine the advantages and disadvantages of classifying information;
- determine a point in time or an event at which declassification should occur; and
- apply "reasoned judgment" throughout the classification process.

In Fiscal Year 1993, there were a total of 1,613 DoD Original Classification Authorities, 782 of them in the NCR. Those Original Classification Authorities made 78,942 original classification decisions, approximately one percent of all classification decisions made during that year. The remaining 7,038,645 classification decisions made during that year were derivative.

**Well-Defined Methodology for Classification**

The guidance on the classification process provided in DoD 5200.1-R presents a well-defined methodology for classification decision-making that we were able to model as shown here.

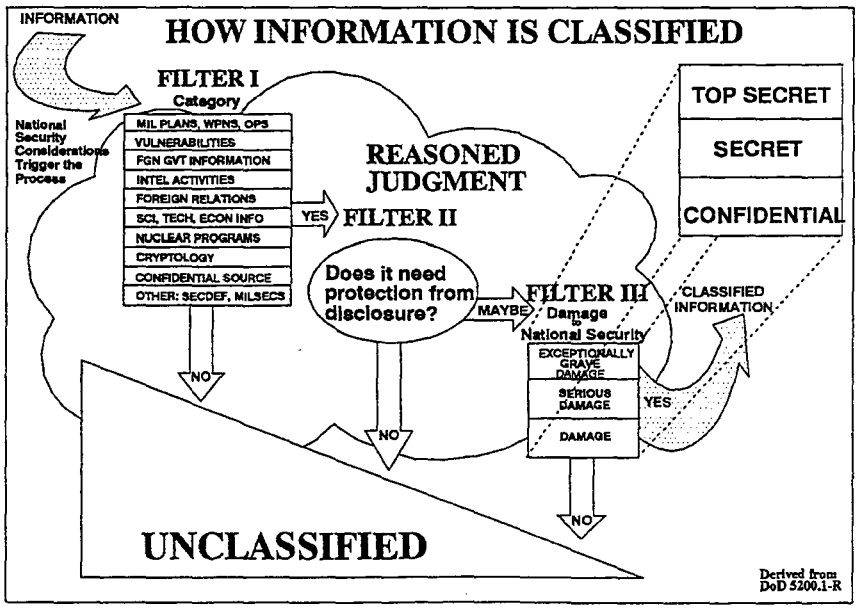


**Figure 1**

Triggered by national security considerations, that decision methodology takes the classifier through three stages. First, the information must fall within ten specific categories. Second, the classifier must determine if the information needs protection in the interests of national security. And, third, if the information needs protection in the interests of national security, the classifier must determine the level of damage to the national security that unauthorized disclosure of the information might cause and assign it a level of classification accordingly. At each stage, the classifier is directed to make decisions based on "reasoned judgment."

**Derivative Classification Process**

Once an original classification decision is made, subsequent classification decisions related to that same information are termed derivative. To accomplish the derivative classification process, DoD 5200.1-R establishes two procedures:

*Security Classification Guides*

- The first procedure is the application of standards in pertinent security classification guides to minimize the need for repeated original classification decisions. DoD 5200.1-I, "Index of Security Classification Guides," September 1994, lists 1,898 currently active security classification guides published by Original Classification Authorities throughout DoD. The oldest of those active guides is dated March 1977, the newest is dated November 1994.

*Classification Based on Existing Classified Information*

- The second and more common procedure is the extraction of classified information from one or more classified sources and incorporating that information into another product. The new material is derivatively classified at the same classification level as the source information. Derivative classifiers must respect original classification decisions, attempt to verify the information's current level of sensitivity, and carry forward all protective markings. The ability of derivative classifiers to verify the information's sensitivity is severely limited when the source material is marked, "Classified by: Multiple Sources."

**Summary of the Classification Process**

The results of our interviews suggest that the classification process functions as intended. The policies guiding the classification process are comprehensive and clearly stated. Original Classification Authorities classify information based on "damage to national security standards," using reasoned judgment, while derivative classifiers routinely and automatically do so based on legitimate source materials and security classification guides. DoD personnel within the NCR comprehend and comply with the intent to protect information.

However, those same interviews consistently indicated that both the declassification process and one oversight mechanism, the statistical reporting process, need improvement. Therefore,

we focused our primary analysis on the declassification process and required annual statistical reporting.

# PART III - THE DECLASSIFICATION PROCESS AND OVERSIGHT MECHANISMS NEED IMPROVEMENT

**THE PUBLIC'S RIGHT-TO-KNOW**

While the classification process clearly is focused on the first purpose of the Program, to protect sensitive information, the downgrading and declassification process supports the second goal of the Program--the right of the public to know about DoD operations consistent with the need to protect national security. DoD 5200.1-R establishes the policies guiding the declassification process and provides only three declassification criteria:

**Declassification Criteria**

- information may be downgraded or declassified as soon as national security considerations permit;
- decisions shall be based on the loss of sensitivity of the information with the passage of time or the occurrence of an event that permits declassification; and
- information that continues to meet the classification requirements of DoD 5200.1-R despite the passage of time will continue to be protected.

The results of our interviews show that, given those criteria alone, DoD personnel within the NCR rarely downgrade or declassify information. Further, there is a reluctance to end the protection afforded to information that was easily classified.

## THE DECLASSIFICATION PROCESS

**DECLASSIFICATION AUTHORITIES**

Since the Program's emphasis on protection far overshadows the public's right to know, we found that the downgrading and declassification process (hereafter referred to simply as the declassification process) established by DoD 5200.1-R is neglected. Similar to the restriction of classification authority to a selected number of specifically designated officials, declassification authority is also restricted to the incumbents of specific positions.

The Secretary of Defense, the Secretaries of the Military Departments, the official who authorized the original classification or persons officially designated as declassification authorities, may downgrade and declassify classified information. Declassification authorities, designated as such by Original Classification Authorities, are "additional officials at the lowest practicable echelons of command and supervision to exercise declassification and downgrading authority over classified information in their functional areas of interest."

As of 1993, Original Classification Authorities had designated 166 additional declassification authorities in the DoD, 95 percent of them in the Military Services. However, Program managers in each of the Services advised us that those authorities, fulfilling the responsibilities as an additional duty, do not routinely declassify information. They almost always act in response to specific requests, usually initiated under the Freedom of Information Act. In most cases, they consult with an Original Classification Authority or subject matter expert before making a decision to declassify. Thus, additional declassification authorities have little impact on the declassification process.

**DECLASSIFICATION UNDER DoD 5200.1-R**

DoD 5200.1-R specifies that, at the time of its creation, all originally or derivatively classified material is to be marked with declassification instructions, either a specific date or event that will trigger declassification or the notation that the "Originating Agency's Determination is Required (OADR)." The results of our interviews revealed that DoD personnel within the NCR consistently and routinely apply the OADR marking since the greatest amount of classified material cannot be associated with a date or event for declassification.

**OADR--The Default Marking**

Declassification is triggered by specific dates or events only in isolated instances such as at the conclusion of a Secretary of Defense overseas travel itinerary, or at the conclusion of a specific military exercise. Because classifiers use the OADR declassification marking instead of determining specific dates or events for declassification, declassification occurs rarely.

The DoD Information Security Program Data Report for Fiscal Year 1993 reflected that of 78,942 original classification decisions, 75,469, or 95.6 percent, were marked OADR, and the May 1993 GAO report stated that classified documents designated OADR government-wide increased from 65 percent in 1984 to 95 percent by 1992.

The OADR marking requires potential declassifiers to consult the originating agency. However, based on our interviews, such requests are rare. Rather than requesting determinations, as required by the OADR declassification marking, our interviews reveal that most DoD personnel opt to simply destroy rather than declassify material. Even mandatory and systematic declassification reviews contribute little to either the declassification effort or the reduction of classified holdings. For example, the DoD Information Security Program Data Report for Fiscal Year 1993 reflected that of 10,279,356 pages reviewed for declassification, only 25.9 percent were declassified.

**Mandatory Declassification Reviews**

DoD 5200.1-R stipulates that mandatory declassification reviews may be requested by any U.S. citizen or permanent resident alien, a federal agency, or a state or local government, generally under the provisions of the Freedom of Information Act. Our interviews disclosed that requests for reviews under the Freedom of Information Act provide the only incentive to

declassify information. A reason for lack of incentive is that declassification reviews involve a manpower intensive, time-consuming line-by-line analysis of classified information. We found line-by-line analysis is a strong deterrent to routine declassification. We believe that the recurring high turnover of DoD personnel within the military services is an additional deterrent to routine declassification. Newly arrived personnel, lacking familiarity with the classified information on hand, may be reluctant to declassify information.

**Systematic Declassification Reviews**

DoD 5200.1-R also mandates a systematic declassification review of the 30-year-old permanently valuable records and 50-year-old intelligence and cryptographic records created after 1945 held by the National Archives and Records Administration. That review, the responsibility for which rests with the Archivist of the United States, is conducted with the assistance of DoD personnel. Since it is not actually a DoD responsibility, we did not look into the archives review process.

## DISSEMINATION OF DECLASSIFICATION NOTICES

When declassification occurs, DoD 5200.1-R requires that all original holders be notified of the downgrading or declassification action. While notification of original holders may be possible, further dissemination of such notices to any additional holders of that information is not all encompassing. Holders of TOP SECRET information can be notified only because there is continuous accountability of who had access to the TOP SECRET information. However, there is no accountability of who holds the SECRET and CONFIDENTIAL information that constitutes the greatest percentage of DoD's classified holdings.

Moreover, if the information has been incorporated into other derivatively classified products, it is nearly impossible to identify the holders of those additional products. As a result, information downgraded or declassified by an originating agency may remain classified indefinitely since there is no mechanism to determine who is in possession of that derivatively classified information.

**Impact of Reproduction and Facsimile Machines**

The difficulties associated with dissemination of declassification notices are magnified when multiple copies of classified documents are produced and distributed. The reproduction of classified documents in support of routine staffing actions by copying and facsimile machines further magnifies the volume of classified holdings throughout the DoD. The wider distribution of reproduced and facsimile copies of classified information reduces the likelihood that holders of that information will receive declassification notices. The result is what the Joint Security Commission called "an enormous backlog of potentially declassifiable information" that amounts to several hundred million pages, with millions of pages being added each year.

**Impact of Office Automation**

The difficulties associated with reproduction and facsimile machines are similar to the difficulties presented by sophisticated office automation systems and networks. The advent of those

systems and networks provides the option of a "paperless environment," in which classified information is created, processed, managed and stored electronically. As in the case of reproduction and facsimile machine transmissions discussed above, electronically stored classified information can be easily and quickly duplicated, resulting in multiple copies. Likewise, such information can be transmitted electronically to multiple addressees, again creating multiple copies.

However, while such multiple copies are created and transmitted regularly, automation systems and networks offer two advantages: the potential elimination of multiple copies of printed classified documents and the expedited staffing of classified actions through electronic mail. Both would contribute to a reduction of classified holdings throughout the DoD. Any printed copies created would be "working papers," which should be destroyed when no longer needed. Finally, permanent record storage would be via electronic media, greatly increasing the capacity of existing storage containers or vastly reducing the requirement for such containers.

*Automation System Constraints*

However, despite the obvious appeal of the automation systems and networks, there are constraints. First, availability and compatibility of such automation systems or networks varies throughout the DoD. Second, any system used to process classified information must be accredited for that purpose, and meet a variety of security requirements. Among those requirements are maintaining the integrity of all system hardware and supporting software; maintaining the integrity of all electronically stored classified data files; and ensuring proper access controls are in place for each such system or network as well as the classified information stored within.

*Potential Drawbacks to Automation Systems*

In conjunction with those practical and security limitations, there are some practical drawbacks to automation. Electronic storage media, particularly magnetic media, deteriorate over time. Magnetic fields eventually collapse, and if classified information is stored on such a medium, it would be corrupted or lost by that collapse. To overcome this drawback, electronically archived classified information would require periodic backup on new storage media. An obvious alternative is the retention of a single hard copy of each classified file stored on the electronic storage media.

*An Opportunity for the Future*

Despite the difficulties and limitations of automated systems and networks, continuing refinements and compliance with procedural requirements provide an opportunity for the future. In conjunction with those refinements, we suggest that DoD automation managers consider methods to incorporate declassification considerations into any system accredited for processing classified information. However, those declassification considerations must evolve from an effective declassification process.

**DECLASSIFICATION PROCESS WORKS ONLY ON DEMAND**

As structured, the declassification process does not work as intended. The Joint Security Commission reached the same conclusion. The near universal use the "OADR" declassification marking delays the start of the declassification process. That delay is the single largest cause of the vast store of existing classified information.

We believe there are three reasons why the declassification process is ineffective:

**Guidance to Accomplish Declassification Inadequate**

- First, the process is ineffective because the guidance that supports it is inadequate in two respects.
  - The first is the authorization to use "OADR" as the declassification marking. Both Executive Order 12356 and DoD 5200.1-R direct that declassification instructions be assigned at the time information is classified. The guidance intends that the declassification process begin at the same point the classification process does, with the Original Classification Authority. By allowing the Original Classification Authority to defer a declassification determination, the "OADR" option delays indefinitely--if not permanently--the declassification process.
  - The second is the lack of guidance for decision making that supports the declassification process. The three declassification criteria provided by DoD 5200.1-R are not adequate alone.

**Program Influenced By Risk Avoidance**

- Second, the Information Security Program, like all security programs, is influenced by a *risk avoidance* philosophy. The Joint Security Commission described risk avoidance as a philosophy which postulates an all-knowing, highly competent enemy that must be countered by minimizing vulnerabilities and maximizing defensive mechanisms as the underlying basis for security decisions. We believe that the influence of risk avoidance works to perpetuate indefinitely classified material and also leads Original Classification Authorities to use the "OADR" marking. That same approach also leads agencies to insist on line-by-line reviews and reject blanket or automatic declassification to avoid risking any loss of information.

**Little or No Incentive to Declassify**

- Finally, there is no incentive to declassify information. Participants in the Program are given a clear motive for classifying information and the consequences of unauthorized disclosure are repeatedly emphasized. There is no similar incentive for declassifying information. In fact, the risk avoidance philosophy and the Program emphasis on protection work as disincentives, generating great reluctance to declassify. Without that incentive,

Program participants developed other ways to control, if not reduce, classified inventories.

## REDUCTION OF CLASSIFIED INVENTORIES

There are two existing techniques to reduce the inventories of classified holdings: destruction and the publication of unclassified replacement products. There are both advantages and disadvantages to these approaches.

### Destruction of Classified Holdings

Our interviews indicate that destruction of unnecessary classified holdings is the default means to reduce those holdings. Destruction is easily implemented and eliminates the potential for premature or improper declassification. We believe that several refinements in DoD 5200.1-R could contribute to the effective reduction of classified holdings through destruction:

- Include a clear definition of "permanently valuable DoD records" in DoD 5200.1-R.
- Require Original Classification Authorities to specify a particular "Office of Record" for each classified document created. By doing so, Original Classification Authorities ensure that future derivative classifiers can verify the sensitivity of the information, particularly when the information has been incorporated into derivatively classified documents bearing the marking, "Classified by: Multiple Sources."
- Require derivative classifiers to cite the "Office(s) of Record" identified in classified source materials when derivatively classifying documents.

Implementing these refinements would have the following benefits:

- Any classified document not determined to be a "permanently valuable record of the DoD" could be routinely destroyed.
- Any office, other than the "Office of Record" for a classified document, could routinely destroy classified holdings that are no longer needed without fear of destroying a "permanently valuable record of the DoD."
- Any derivatively classified information for which a DoD activity is not the "Office of Record" could be destroyed when no longer needed.
- Designation of an "Office of Record" should help derivative classifiers verify the current sensitivity of information contained in classified source materials marked "Classified by: Multiple Sources."

The combined result of these suggested refinements should be a reduction in the total of classified holdings, especially those that

are mere duplications of material held elsewhere throughout the DoD. Destruction of unneeded classified holdings, however, is not without its limitations. First, "permanently valuable DoD records," routinely transferred to the National Archives and Records Administration, are not eligible for destruction. Additionally, those records are not considered for declassification until they are at least 30 years old. Second, destruction does not support the second goal of the Program, and perpetuates risk avoidance and the status quo.

**Publication of Unclassified Replacement Products**

The Defense Mapping Agency publishes new, unclassified replacement products for existing classified products, the second technique to control classified holdings. This technique also eliminates problems with the dissemination of declassification notices. However, the approach is time-consuming and labor intensive. Further, the publisher cannot be assured that all holders of the original classified products will receive the unclassified replacement products.

Despite the importance of traditional techniques to control classified inventories, more must be done. Those inventories, as described by the Joint Security Commission, continue to grow by "millions of pages each year." Our analysis suggests that meaningful reductions of those classified inventories could be achieved by improving the declassification process. We believe there are three reasons the declassification process itself needs improvement (e.g., inadequate guidance, risk avoidance, and little or no incentive to declassify). To provide declassifiers the tools they now lack, and give Original Classification Authorities a tool they need to make declassification decisions at the time of classification, we suggest the following three steps.

## DECLASSIFICATION DECISION-MAKING

We believe the first change needed is to provide adequate guidance to support the declassification process. We propose that there are two alternative methodologies to improve the declassification process: either a checklist to guide declassifiers or a new, clearly defined declassification procedure. There are advantages and disadvantages to both these alternatives.

**Include A Declassification Checklist**

As a first alternative, we suggest that the DASD(I&S) consider incorporating the declassification guidance and criteria currently provided in Enclosures 2, 4, 5, and 6, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983, in DoD 5200.1-R (See Appendix E). That guidance, although focused on "permanently valuable DoD records," may assist DoD Original Classification Authorities and additional declassification authorities determine when information can and should be declassified.

**Incorporate A Clearly Defined Declassification Methodology**

As a second alternative, we offer a prototype declassification decision-making procedure, based on the classification methodology (Figure 2). Unlike the full treatment of the classification decision-making methodology provided in DoD 5200.1-R and

depicted in Figure 1, page 8, Part II, the existing guidance on the declassification process does not address the issue of how to declassify. Our proposal is intended to change the way DoD personnel think about the declassification process, an essential step to implement this alternative. The modeled conditions are illustrative, not definitive.

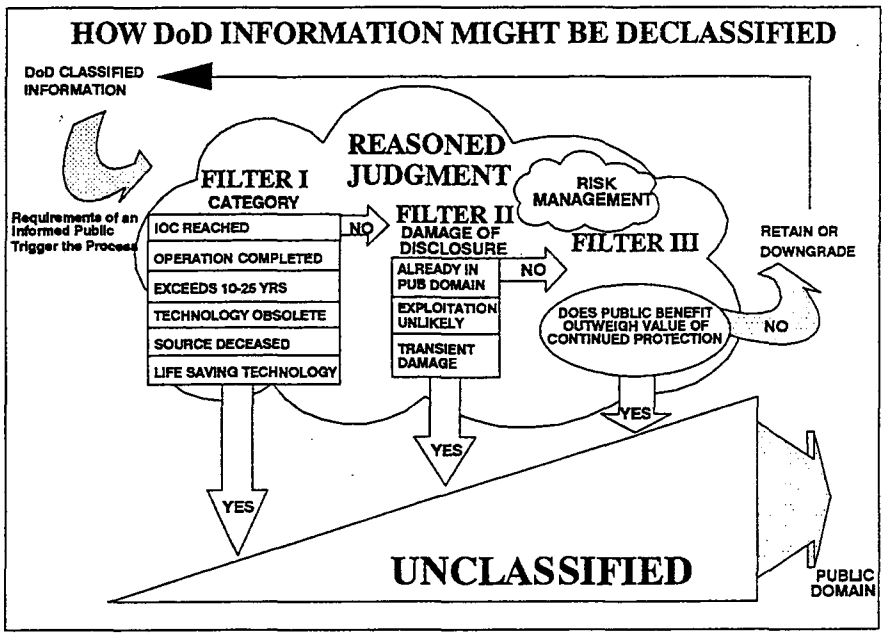


**Figure 2**

We constructed a procedure that takes the declassifier through three decision points. First, if the classified information meets one or more specific, clear-cut conditions it may be declassified by any Original Classification Authority unilaterally (Filter I). If it does not, a declassification authority must apply risk management to determine whether disclosure would damage national security (Filter II). If it is determined that little or no damage will result from disclosure, the information may be declassified. If it is decided disclosure might cause damage, the declassifier must again apply the principles of risk management to determine if the benefit to the public outweighs the value of continued protection and declassify it if that is the case (Filter III). As in the case of classification decisions, the declassifier must make the choice at each decision point based on reasoned judgment.

If this alternative is selected, we suggest the DASD(I&S) expand DoD 5200.1-R to include a readily identifiable, logical and clearly defined declassification decision procedure resembling the prototype procedure illustrated in Figure 2.

**Summary of Alternatives**

Selection of either alternative will provide declassifiers the essential guidance they now lack, and give Original Classification Authorities a tool they need to make the initial declassification

decision at the time of classification. Finally, either alternative will improve the balance of the classification-declassification system by providing the same specificity for declassification decisions that is now provided for classification decisions. However, we believe that the checklist approach to declassification provided in DoD Directive 5200.30 and Appendix E may be cumbersome and inefficient. The existing checklist is long, addresses a multitude of information categories in generalized terms, and provides no methodology to support the declassification process. Therefore, we suggest that the prototype declassification model may be a preferred approach because of its simplicity and ease of interpretation. In fact, DoD Program managers could use both alternatives concurrently and provide improved declassification guidance and a clearly defined declassification procedure.

**EXPAND AND REVISE DECLASSIFICATION GUIDANCE**

If the declassification decision methodology alternative provided in Figure 2 is selected, we suggest that the guidance on declassification be revised and expanded. Two changes would be needed:

- limit the life of classified information by eliminating the default marking for declassification of "OADR;" and
- establish a specific period of time after which the information is declassified without review.[2] Original Classification Authorities must be required to make a downgrading or declassification decision of some kind at the time they classify the information.

**Risk Management Philosophy Must be Adopted**

Regardless of which alternative is selected, we believe another change needed to make the declassification process work is the adoption of risk management as the operating philosophy underlying the DoD Program. Rather than the "worst case" approach of risk avoidance, risk management postulates that it is possible to balance the risk of disclosure against the costs of protection in terms of dollars and efficient information flow. Changing an operating philosophy is not an easy task; the change cannot be imposed, only introduced, encouraged and supported. It will take several years for the influence of risk management to spread throughout DoD. However, its adoption by the Program participants is essential if the steps we suggest are to be effective. The risk management concept must be included in DoD Directive 5200.1 and the principles of risk management discussed in DoD 5200.1-R. Program instruction conducted throughout the DoD should also reflect the risk management philosophy.

**Develop Incentives to Declassify**

Our research indicates that one final step to improve the declassification process is the development of a stronger incentive for declassification. Program participants must recognize that the

[2] Executive Order, 12958, "Classified National Security Information," April 17, 1995, eliminated "OADR" and established a specific time frame after which declassification would occur without review.

administrative impact of protecting, handling, processing and transmitting classified information has a negative impact on the operational efficiency of their organization. Once DoD personnel understand the impact of classification, they may be more likely to see the benefits of declassifying information whenever possible.

**Summary of the Declassification Process**

We believe that the declassification process is the weakest element of the classification-declassification system. The process needs improvement for the following reasons:

- guidance fails to provide a methodology for declassification decision-making;
- the influence of risk avoidance perpetuates indefinitely classified information, and reinforces a reluctance to declassify information;
- Original Classification Authorities defer declassification decisions indefinitely through the widespread use of OADR;
- most DoD personnel opt to simply destroy rather than declassify classified material; and
- even in the rare instances when declassifications do occur, notification of all holders of the information that declassification has occurred is not realistic.

## OVERSIGHT MECHANISMS

The final component of the classification-declassification system, oversight mechanisms, are the tools and techniques that Departmental managers employ to ensure implementation of established Program policies and procedures. We identified four oversight mechanisms that support the Program: management actions, training, challenges to classification decisions, and statistical reporting. Results of our interviews indicate that management actions and training, while essentially sound, focus primarily on the protective aspects of the Information Security Program. Our interviews also indicate that informal and infrequent challenges to classification decisions occur, meeting established standards. However, results of our interviews and our analysis of the DoD Information Security Program Data Report for Fiscal Year 1993 indicate that statistical reporting is ineffective. We focus, therefore, solely on statistical reporting.

**ANNUAL REPORTING REQUIREMENT**

DoD 5200.1-R directs DoD activities to submit Standard Form (SF) 311, "Agency Information Security Program Data," annually (see Appendix D). DoD activities may chose to submit data based either on a sampling technique or cumulative totals for the reporting period. All SF 311s prepared by DoD activities are

into a single SF 311 by DoD Program Managers. The consolidated SF 311 is then forwarded to the Information Security Oversight Office (ISOO). The ISOO incorporates the DoD input into the "Information Security Oversight Office Annual Report to the President," required by Executive Order 12356. The SF 311 contains data on a variety of classification-declassification activities, such as the number of original and derivative classifications made, the number of pages systematically reviewed and declassified, and the number of infractions involving overclassification and underclassification.

**Reported Data Not Meaningful**

We determined initially through interviews, but ultimately through our analysis of the Fiscal Year 1993 SF 311 submissions, that while statistical data is reported by DoD activities, it is unreliable, both qualitatively and quantitatively. Other than levying the requirement for an annual report, DoD 5200.1-R provides no guidance on what is to be reported. With no guidance to support the process, and no uniformity in the data reported, there is uncertainty over what the data represents. The SF 311 itself only provides brief, general instructions that are open to wide interpretation on what is to be reported and how reported information should be categorized. Further, the SF 311 establishes no requirement to report the impact of copier machines on the volume of classified holdings.

**No Standardized Sampling Technique**

There is no standardized sampling technique. Multiple sampling techniques further complicate the process. For the Fiscal Year 1993 report, three different sample patterns (one four-week period, two two-week periods, and four one-week periods) were used; sample periods ranged from February through September. The aggregation of data collected using varied sampling techniques reduces the accuracy and reliability of the data reported.

Our interviews indicate that the security specialists who compile the SF 311s perceive the report as an external requirement rather than an internal management tool. They generally perform no quality control, and conduct little or no analysis of the data. Their goal is simple quantification to satisfy the requirement. That perception is one reason for that lack of accuracy and reliability. To illustrate the magnitude of the problem, the data submitted to DoD by all subordinate activities reflected that those activities had originally and derivatively classified a total of 7,038,645 documents. However, the consolidated DoD report to ISOO reflected original and derivative classifications totaling only 4,067,681.

**Perception Contributes to Confusion**

Program managers in each of the Military Departments acknowledged that they were not sure what the data in certain sections of the SF 311 actually represented. For example, Block 7 of the SF 311 requires activities to report original and derivative classification decisions, but provides no guidance as to what constitutes such decisions (e.g., a paragraph, a page, a document, a collection of documents, a computer record or file

could each represent an original classification decision, and every DoD activity could compile the data differently). As a result of Program managers lacking confidence in the data reported on the SF 311, they make little or no use of it.

**Guidance Lacking**

The lack of clear guidance and standardized sampling techniques led some we interviewed to suggest that the annual SF 311 report be eliminated. However, statistical reporting can provide useful indications of Program activity, identify trends, and highlight potential problems requiring management attention. Additionally, implementation of Government Performance and Results Act requires increasingly precise measurement, not less. To provide that reliable measurement, we suggest that the DoD Security Institute be tasked to develop rigorous reporting criteria to be included in DoD 5200.1-R. Once guidance is clarified, statistical reporting can more closely approach an actual, rather than potential, oversight mechanism. Finally, we believe that DoD Program Managers should designate a single, common sampling period that varies year by year for all Department of Defense activities.

## SUMMARY AND CONCLUSIONS

The conclusion that there is too much classified information is a long-standing one, and the pressure to reduce the volume of classified information has grown steadily in recent years. Based on our analysis, we conclude that the present size of classified holdings is the result of too much information remaining classified for too long. Because the Program puts little emphasis on declassification, efforts made to declassify information are insufficient. The declassification process suffers from weaknesses that seriously impair its operation. Risk avoidance contributes to the perpetuation of indefinitely classified information. The incentives to declassify information are inadequate, and the supporting guidance is inadequate. Program managers and participants have lost sight of the fact that the program is twofold--to safeguard information from unauthorized disclosure for national security reasons and to satisfy the right of the public to know.

Of necessity, the Program has put great emphasis on the need to protect classified information, but in doing so, has neglected the needs of an informed public. A better balance needs to be achieved. Risk management can be applied to the Program and greater weight can be given to the right of the public to know without additional risk to forces and plans.

Many of the recent proposals to reduce the volume of classified information have concentrated on the review and declassification of information in the National Archives. That is a necessary effort, but it does not represent a long-term solution to the problem. In the long term, the problem must be attacked

at the working level, not in the archives. That means that declassification must be just as much of a routine, day-to-day practice among Program participants as classification is today. DoD can take the lead in implementing that long-term solution by re-orienting the Program to accord greater emphasis to the needs of an informed public.

# APPENDIX A
# RELEVANT POLICY DOCUMENTS AND REFERENCES

| | |
|---|---|
| **AFP 205-37** | Air Force Pamphlet 205-37, "Preparing Security Classification Guides," November 5, 1991 |
| **AFR 205-1** | Air Force Regulation 205-1, "Information Security Program Regulation," April 28, 1987 |
| **AI-26** | Deputy Assistant Secretary of Defense (Administration) Administrative Instruction #26, "Information Security Supplement to DoD 5200.1-R," April 1, 1987 |
| **AR 380-5** | Army Regulation 380-5, "Department of the Army Information Security Program," February 25, 1988 |
| **DIAR 50-2** | Defense Intelligence Agency Regulation 50-2, "Information Security Program," July 15, 1993 |
| **DoD 5200.1** | Department of Defense Directive 5200.1, "DoD Information Security Program," June 7, 1982 |
| **DoD 5200.1-H** | Department of Defense Handbook 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 18, 1986 |
| **DoD 5200.1-I** | Department of Defense Index 5200.1-I, "Index of Security Classification Guides," September, 1994 |
| **DoD 5200.1-PH** | Department of Defense Handbook 5200.1-PH, "A Guide to Marking Classified Documents," November 1982 |
| **DoD 5200.1-R** | Department of Defense Regulation 5200.1-R, "Information Security Program Regulation," June 1, 1986 |
| **DoD 5200.30** | Department of Defense Directive 5200.30, "Guidelines for Systematic Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983 |
| **DoD O-5210.85** | Department of Defense Instruction O-5210.85, "Umbrella Security Classification Guide for High Technology Information," April 27, 1993 |
| **DoD 5400.7** | Department of Defense Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980 |
| **DLAR 5200.12** | Defense Logistics Agency Regulation 5200.12, "DLA Information Security Program," June 22, 1987 |
| **EO 12356** | Executive Order 12356, "National Security Information," April 2, 1982 |

| | |
|---|---|
| **EO 12958** | Executive Order 12958, "Classified National Security Information," April 17, 1995 (supersedes EO 12356) |
| **ISOO DIRECTIVE #1** | Information Security Oversight Office Directive #1, "National Security Information," June 23, 1982 |
| **JAI 2511.03P** | Joint Administrative Instruction 2511.03P, "Joint Staff Information Security Program," May 13, 1991 |
| **OPNAVINST 5510.1H** | Chief of Naval Operations Instruction 5510.1H, "Department of the Navy Information and Personnel Security Regulation," April 29, 1988 |
| **OPNAVINST 5513.1D** | Chief of Naval Operations Instruction 5513.1D, "Department of the Navy Security Classification Guides," February 24, 1989 |
| **REFERENCE DOCUMENTS** | "Department of Defense Information Security Program Data Report, October 1, 1992-September 30, 1993," Annual Report to the Information Security Oversight Office |
| | "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence," Joint Security Commission, February 28, 1994 |
| | "Report of the Commission on Government Security," U.S. Government Printing Office, Washington, D.C., June 21, 1957 |
| | U.S. General Accounting Office Report to Congressional Requestors, "CLASSIFIED INFORMATION: Volume Could Be Reduced by Changing Retention Policy," GAO/NSIAD-93-127, May 1993 |

# APPENDIX B
# ACTIVITIES VISITED

| | |
|---|---|
| **OSD** | Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) |
| | Department of Defense Security Institute |
| | Office of the Director, Administration and Management, Washington Headquarters Services |
| | Office of the Inspector General, Department of Defense |
| | Office of the Under Secretary of Defense for Acquisition and Technology |
| | Office of the Under Secretary of Defense for Policy |
| **THE JOINT STAFF** | Office of the Director for Information and Resource Management |
| **DEFENSE AGENCIES** | Ballistic Missile Defense Organization |
| | Defense Information System Agency |
| | Defense Intelligence Agency |
| | Defense Logistics Agency |
| | Defense Mapping Agency |
| | Defense Nuclear Agency |
| | National Security Agency |
| | On-Site Inspection Agency |
| **MILITARY DEPARTMENTS** | Department of the Army |
| | Department of the Navy |
| | Department of the Air Force |
| | U.S. Marine Corps |

# APPENDIX C
# TEAM MEMBERS

Mr. Frank Griggs
**Project Director**

Mr. William Cogley
**Project Assistant**

Mr. Miles Kara
**Project Assistant**

Ms. Nakita Pounds
**Project Coordinator**

# APPENDIX D
# STANDARD FORM 311, AGENCY INFORMATION SECURITY PROGRAM DATA REPORT

*(IMPORTANT - Read instructions on reverse before completing this form)* OMB NO. 3090-0

| AGENCY INFORMATION SECURITY PROGRAM DATA | 1. PERIOD COVERED A. FROM | B. TO | INTERAGENCY REPORT CONTROL NUMBER |
|---|---|---|---|
| | | | 0230-GSA-AN |
| 2. DEPARTMENT, INDEPENDENT AGENCY OR ESTABLISHMENT | 3. CONTACT FOR ADDITIONAL INFORMATION *(Name, office and telephone no.)* | | |
| 4. SENIOR OFFICIAL *(Section 5.3, E.O. 12356)* | | | |

| 5. NUMBER OF ORIGINAL CLASSIFICATION AUTHORITIES | | | |
|---|---|---|---|
| A. TOP SECRET | B. SECRET | C. CONFIDENTIAL | D. TOTAL |
| | | | |

| 6. ADDITIONAL DECLASSIFICATION AUTHORITIES | | | |
|---|---|---|---|
| A. TOP SECRET | B. SECRET | C. CONFIDENTIAL | D. TOTAL |
| | | | |

| 7. CLASSIFICATION DECISIONS | ORIGINAL | | DERIVATIVE |
|---|---|---|---|
| | DATE OR EVENT (a) | ORIGINATING AGENCY'S DETERMINATION REQUIRED (O.A.D.R.) (b) | (c) |
| A. TOP SECRET | | | |
| B. SECRET | | | |
| C. CONFIDENTIAL | | | |

| 8. MANDATORY REVIEW REQUESTS AND APPEALS | CASES FOR WHICH AGENCY IS RESPONSIBLE FOR FINAL DECISION | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | CASES CARRIED OVER FROM PREVIOUS PERIOD (a) | NEW CASES RECEIVED (b) | DECLASSIFICATION DECISIONS *(Report in cases, documents, and pages)* | | | | | | | | CASES CARRIED OVER TO NEXT PERIOD (f) |
| | | | GRANTED IN FULL (c) | | | GRANTED IN PART (d) | | | DENIED (e) | | |
| | | | CASES | DOCS. | PAGES | CASES | DOCS. | PAGES | CASES | DOCS. | PAGES | |
| A. REQUESTS | | | | | | | | | | | | |
| B. APPEALS | | | | | | | | | | | | |

| 9. SYSTEMATIC REVIEW FOR DECLASSIFICATION *(In pages)* | | 10. NUMBER OF FORMAL INSPECTIONS, SURVEYS, OR PROGRAM REVIEWS |
|---|---|---|
| A. REVIEWED | B. DECLASSIFIED | |
| | | |

| 11. NUMBER OF INFRACTIONS INVOLVING: | | | | | |
|---|---|---|---|---|---|
| A. OVERCLASSIFICATION | B. UNDERCLASSIFICATION | C. CLASSIFICATION WITHOUT AUTHORITY | D. MISMARKING | | |
| | | | | | |
| E. IMPROPER DESTRUCTION | F. UNAUTHORIZED ACCESS | G. IMPROPER STORAGE | H. IMPROPER REPRODUCTION | I. IMPROPER TRANSMISSION | J. OTHER *(Elaborate under Item 12)* |
| | | | | | |

12. REMARKS

311-102

STANDARD FORM 311 (REV. 4-83)
Prescribed by GSA/ISOO
E.O. 12356

## INSTRUCTIONS

1. GENERAL

This reporting requirement applies to each department, independent agency or establishment in the executive branch that creates, handles, and/or stores national security information. The reporting period is on a fiscal year basis, except for the reporting period of August 1, 1982 through September 30, 1983. Submissions must be unclassified and typewritten, and reach ISOO no later than October 31 following the reporting period. Consolidate the submissions of component activities into a single report. Agencies, however, shall retain the input from component activities for possible ISOO review.

II. SPECIFIC

Item 5. Enter the number of "Top Secret," "Secret," and "Confidential," original classifiers. Enter only the highest level authorized; i.e., enter the number of individuals with "Top Secret" authority in boxes A and D, only; "Secret" authorities in boxes B and D, only; and "Confidential" authorities in boxes C and D, only.

Item 6. See instructions provided for completing Item 5, above. This entry seeks the number of additional declassification authorities, excluding those original classifiers listed in Item 5.

Item 7. Enter the actual number of original classification decisions made during the reporting period, breaking these down by the classification level and the type of declassification instruction assigned. Enter the actual count of derivative classification decisions by classification level. Do not count reproductions or copies as classification decisions. Agencies that generate a high volume of classification decisions may request, in writing, authorization from the ISOO Director to use sampling methods in lieu of an actual count. Sampling methods already approved may continue in effect until revised.

Item 8. Enter the number of mandatory review requests and appeals carried over from the previous reporting period, new ones received, actions taken on them, and the number of requests carried over to the next reporting period. For purposes of this report: "Case" means an individual mandatory review request or appeal, regardless of the number of requestors cited in the request or the number of documents or pages to be reviewed as a result of the request; "document" means recorded information, regardless of physical format, that has been created or reproduced as an integrated and complete unit; and, "page" means one side or face of recorded information.

Item 9. Enter in box A the number of pages in the agency's custody systematically reviewed for declassification and in box B the number of pages declassified as a result of the review.

Item 10. For purposes of this report, and "inspection, survey, or program review" means any formal, internal evaluation of any aspect of the agency's information security program.

Item 11. An infraction is any error and/or impropriety in marking, destroying, handling reproducing, transmitting, gaining or granting access to or storing classified information. Enter in the appropriate box the number of infractions revealed or detected during the reporting period. Do not included those violations that must be reported to the ISOO Director under section 5.4(b) of the Order.

STANDARD FORM 311 BACK (REV 4-83)

# APPENDIX E
# EXTRACT OF DOD DIRECTIVE 5200.30

## CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION[1]

The following categories of information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Nuclear propulsion information.

2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

3. Information concerning the safeguarding of nuclear materials or facilities.

4. Information that could affect the conduct of current or future U.S. foreign relations. (Also see enclosure 5.)

5. Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operation plans.

6. Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

7. Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

8. Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information that reveals the overall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

9. Information that relates to intelligence activities conducted jointly by the Department of Defense with other federal agencies or to intelligence activities conducted by other federal agencies in which the Department of Defense has provided support. (Also see enclosure 6.)

10. Airborne radar and intercept imagery.

11. Information that reveals space system:

---

[1] Copy of Enclosure 2, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

a. Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

b. Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

12. Information that reveals operational communications equipment and systems:

a. Electronic counter-countermeasures (ECCM) design features or performance capabilities.

b. Vulnerability or susceptibility to any or all types of electronic warfare.

13. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

a. Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

b. Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

14. Information concerning Department of the Army systems listed in attachment 1.

15. Information concerning Department of the Navy systems listed in attachment 2.

16. Information concerning Department of the Air Force systems listed in attachment 3.

17. Cryptologic information (including cryptologic sources and methods). This includes information concerning or revealing the processes, techniques, operations, and scope of SIGINT comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of COMSEC, including the communications portion of cover and deception plans.

a. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

(1) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Many COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing transmission security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC documentation such as National COMSEC Instructions, National COMSEC/Emanations Security (EMSEC) Information Memoranda, National COMSEC Committee Policies, COMSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(2) Those that relate to SIGINT. These appear as reports in the various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains

codeword material: and "Utmost secrecy is necessary..." Formats may appear as messages have addressees, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(3) RDT&E reports and information that relate to either COMSEC or SIGINT.

b. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

Attachments - 3
1. Department of the Army Systems
2. Department of the Navy Systems
3. Department of the Air Force Systems

## CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION DEPARTMENT OF THE ARMY SYSTEMS[2]

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Ballistic Missile Defense (BMD) missile information, including the principle or operation of warheads (fuzing, arming, firing, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM; details of design, assembly, and construction; and principle of operations.

2. BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

4. Shaped-charge technology.

5. Fleshettes.

6. M380 beehive round.

7. Electromagnetic propulsion technology.

8. Space weapons concepts.

9. Radar-fuzing programs.

10. Guided projectiles technology.

11. ECM and ECCM to weapons systems.

12. Armor materials concepts, designs, or research.

13. 2.75-inch Rocket System.

14. Air Defense Command and Coordination System (AN/TSQ-51).

15. Airborne Target Acquisition and Fire Control System.

16. Chaparral Missile System.

17. Dragon Guided Missile System Surface Attack, M47.

18. Forward Area Alerting Radar (FAAR) System.

---

[2] Copy of Attachment 1 to Enclosure 2, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

19. Ground laser designators.

20. Hawk Guided Missile System.

21. Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).

22. Honest John Missile System.

23. Lance Field Artillery Missile System.

24. Land Combat Support System (LCSS).

25. M22 (SS-11 ATGM) Guided Missile System, Helicopter Armament Subsystem.

26. Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANYTIME Improvement).

27. Patriot Air Defense Missile System.

28. Pershing IA Guided Missile System.

29. Pershing II Guided Missile System.

30. Guided Missile System, Intercept Aerial M41 (REDEYE) and Associated Equipment.

31. U.S. Roland Missile System.

32. Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).

33. Shillelagh Missile System.

34. Stinger/Stinger-Post Guided Missile System (FIM-92A).

35. Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).

36. TOW Heavy Antitank Weapon System.

37. Viper Light Antitank/Assault Weapon System.

## CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION DEPARTMENT OF THE NAVY SYSTEMS[3]

The following categories of Navy information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Naval nuclear propulsion information.

2. Conventional surface ship information:

    a. Vulnerabilities of protective systems, specifically:

        (1) Passive protection information concerning ballistic torpedo and underbottom protective systems.

        (2) Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.

        (3) General arrangements, drawings, and booklets of general plans (applicable to carriers only).

    b. Ship-silencing information relative to:

        (1) Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).

        (2) Procedures and techniques for noise reduction pertaining to an individual ship's component.

        (3) Vibration data relating to hull and machinery.

    c. Operational characteristics related to performance as follows:

        (1) Endurance or total fuel capacity.

        (2) Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.

3. All information that is uniquely applicable to nuclear-powered surface ships or submarines.

4. Information concerning diesel submarines as follows:

    a. Ship-silencing data or acoustic warfare systems relative to:

        (1) Overside, platform, and sonar noise signature.

        (2) Radiated noise and echo response.

        (3) All vibration data.

---

[3] Copy of Attachment 2 to Enclsoure 2, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

(4) Seismic, magnetic (including AM), pressure and UEP signature data.

b. Details of operational assignments, that is, war plans, antisubmarine warfare (ASW), and surveillance tasks.

c. General arrangements, drawings, and plans of SS563 class submarine hulls.

5. Sound Surveillance System (SOSUS) data.

6. Information concerning mine warfare, mine sweeping, and mine countermeasures.

7. ECM or ECCM features and capabilities of any electronic equipment.

8. Torpedo information as follows:

a. Torpedo countermeasures devices: T-MK6 (FANFARE) and NAE beacons.

b. Tactical performance, tactical doctrine, and vulnerability to countermeasures.

9. Design performance and functional characteristics of guided missiles, guided projectiles, sonars, radars, acoustic equipments, and fire control systems.

## CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION DEPARTMENT OF THE AIR FORCE SYSTEMS[4]

The Department of the Air Force has determined that the categories identified in enclosure 2 of this Directive shall apply to Air Force information.

[4] Copy of Attachment 3 to Enclsoure 2, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

## DECLASSIFICATION CONSIDERATIONS[5]

1. Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States; and similar events may bear upon the determination of whether information should be declassified. If the responsible DoD reviewed decides that, in view of such circumstances, the public disclosure of the information being reviewed no longer would result in damage to the national security, the information shall be declassified.

2. The follow are examples of considerations that may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

a. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

b. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

c. The information is pertinent to a system that no longer is used or relied on for the defense of the United States or its allies and does not disclose the capabilities or vulnerabilities of existing operational systems.

d. The program, project, or system information no longer reveals a current weakness or vulnerability.

e. The information pertains to an intelligence objective or diplomatic initiative that has been abandoned or achieved and will no longer damage the foreign relations of the United States.

f. The information reveals the fact or identity of a U.S. intelligence source, method, or capability that no longer is employed and that relates to no current source, method, or capability that upon disclosure could cause damage to national security or place a person in immediate jeopardy.

g. The information concerns foreign relations matters whose disclosure can no longer be expected to cause or increase international tension to the detriment of the national security of the United States.

3. Declassification of information that reveals the identities of clandestine human agents shall be accomplished only in accordance with procedures established by the Director of Central Intelligence for that purpose.

4. The NSA/CSS is the sole authority for the review and declassification of classified cryptologic information. The procedures established by the NSA/CSS to facilitate the review and declassification of classified cryptographic information are:

a. COMSEC Documents and Materials

---

[5] Copy of Enclosure 4, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

(1) If records or material in this category are found in agency files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency concerned or by appropriate channels to the following address:

Director
National Security Agency
ATTN: Director of Policy (Q4)
Fort George G. Meade, Maryland 20755

(2) If the COMSEC information has been incorporated into other documents by the receiving agency, referral to the NSA/CSS is necessary before declassification.

b. SIGINT Information

(1) If SIGINT information has been incorporated by the receiving agency into documents it produces, referral to the NSA/CSS is necessary before declassification.

## DEPARTMENT OF STATE AREAS OF INTEREST[6]

1. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

2. Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

3. Statement of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

4. Agreements with foreign countries for use of, or access to, military facilities.

5. Contingency plans insofar as they involve other countries, the use of foreign bases, territory or airspace, or the use of chemical, biological, or nuclear weapons.

6. Defense surveys of foreign territories for purposes of basing or use in contingencies.

7. Reports documenting conversations with foreign officials, that is, foreign government information.

[6] Copy of Enclosure 5, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

## CENTRAL INTELLIGENCE AGENCY AREAS OF INTEREST[7]

1. Cryptologic, cryptographic, or SIGINT. (Information in this category shall continue to be forwarded to the NSA/CSS in accordance with enclosure 4, paragraph 4. The NSA/CSS shall arrange for necessary coordination.)

2. Counterintelligence.

3. Special access programs.

4. Information that identifies clandestine organizations, agents, sources, or methods.

5. Information on personnel under official or nonofficial cover or revelation of a cover arrangement.

6. Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

7. Methods or procedures used to acquire, produce, or support intelligence activities.

8. CIA structure, size, installations, security, objectives, and budget.

9. Information that would divulge intelligence interests, value, or extent of knowledge of a subject.

10. Training provided to or by the CIA that would indicate its capability or identify personnel.

11. Personnel recruiting, hiring, training, assignment, and evaluation policies.

12. Information that could lead to foreign political, economic, or military action against the United States or its allies.

13. Events leading to international tension that would affect U.S. foreign policy.

14. Diplomatic or economic activities affecting national security or international security negotiations.

15. Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

16. Nonattributable activities conducted abroad in support of U.S. foreign policy.

17. U.S. surreptitious collection in a foreign nation that would affect relations with the country.

18. Covert relationships with international organizations or foreign governments.

19. Information related to political or economic instabilities in a foreign country threatening American lives and installations therein.

---

[7] Copy of Enclosure 6, DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983.

20. Information divulging U.S. intelligence collection and assessment capabilities.

21. U.S. and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.

22. Information disclosing U.S. systems and weapons capabilities or deployment.

23. Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.

24. Information on technical systems for collection and production of intelligence, and their use.

25. U.S. nuclear programs and facilities.

26. Foreign nuclear programs, facilities, and intentions.

27. Contractual relationships that reveal the specific interest and expertise of the CIA.

28. Information that could result in action placing an individual in jeopardy.

29. Information on secret writing when it relates to specific chemicals, reagents, developers, and microdots.

30. Reports of the Foreign Broadcast Information Service (FBIS) (--Branch, -- Division) between July 31, 1946, and December 31, 1950, marked CONFIDENTIAL or above.

31. Reports of the Foreign Documents Division between 1946 and 1940 marked RESTRICTED or above.

32. Q information reports.

33. FDD translations.

34. U Reports.