II Rethinking Classification: Better Protection and Greater Openness

To the credit of the 29 departments and agencies that currently possess the authority to classify information, there have been serious efforts in recent years to improve classification management practices. There has been a growing recognition of the need to replace a risk avoidance approach to security, which seeks to anticipate *all* risks in the protection of assets, with a risk management approach, which seeks to concentrate limited resources on those assets the loss of which would have the most profound effect on the national security. Today, fewer individuals are authorized to classify information in the first instance than ever before, and efforts are underway to better ensure that these classifiers are more aware of their responsibilities and are evaluated on their classification decisions. The number of special access programs and compartments designed to provide additional protection beyond that of the Confidential, Secret, and Top Secret levels has been reduced. Progress has been made in moving large quantities of information out of the remaining compartments and programs and into the three classification levels, where it is more easily used by a broader range of "customers." Most importantly, the number of classification actions continues to decline and today is at its lowest point since the Information Security Oversight Office (ISOO) began compiling classification statistics in 1979.[1]

Notwithstanding these efforts and results to date, more information continues to be classified than national security needs require. Risk management continues to be more of a goal than an operative philosophy guiding today's security decisions. Serious questions remain about the process by which classification decisions are made, and about the oversight, training, and accountability of those who make classification decisions. Particularly disturbing is the continued perception among many inside the Government that the current classification system simultaneously fails to protect the nation's core secrets while still classifying too much. Justice Potter Stewart's observation that "when everything is classified, then nothing is classified" remains very relevant today.[2] As long as more information than necessary is classified, the long-term benefits of the progress cited above will be limited—benefits such as the enhanced protection of the nation's core secrets, the cost savings that will come from limiting classification, and the value of the American public knowing about the operations and activities of its government. This is particularly true given the information explosion in which the amount of data overall will increase dramatically in the years ahead.

If the progress already made is to continue, there must be a renewed focus on the all-important initial decision of whether to classify at all. Avoiding unnecessary classification in the first place should allow for a more efficient use of already-limited resources by focusing on that which truly needs protection. Combined with the proper implementation of classification practices, this also should lessen the burden of subsequent declassification efforts, contributing to a more orderly and cost-efficient review

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

and release of information to the public. And finally, a more thoughtful and balanced consideration of the need for secrecy should enable government officials to better understand the importance of a particular piece of information and why it needs to be protected, leading to enhanced safeguarding of the nation's secrets.

This chapter describes the current classification system and recent improvements to it, and highlights those areas that the Commission finds most ripe for attention as the decades-old struggle between secrecy and openness proceeds into the Information Age. Commission recommendations in this area attempt to reorient the classification decisionmaking process from one that perpetuates a "default" to classification, in which personnel tend to classify more by rote than by reason, to one that involves a more balanced assessment of the need for secrecy.

Toward a Life Cycle Approach to Classification Management

A meaningful assessment of the need for protection over the long term requires revisiting the initial decision to classify throughout the period in which the information is of value (i.e., throughout the life cycle of that information). Viewing information, and the records in which that information is contained, as having a "life span" is not a novel approach. The Information Resources Management Service of the General Services Administration, for example, maintains that "each type of record has its own distinct life cycle; records are born, reproduced, . . . processed, consulted, reviewed, sent to the sidelines, brought back for consultation, may be reborn into another document, and eventually end up in the trash or permanent storage."[3] Likewise, in developing policy for its management of electronic records, the National Archives and Records Administration incorporated "traditional records management theory . . . reflecting the life cycle of records—creation and receipt, maintenance and use, and disposition."[4]

Such management concepts, however, have been applied only to very limited areas of the Government. The various stages of the life cycle still often are viewed as distinct from one another with respect to the management of classified information. The disjointed nature of current information management practices has a range of troubling consequences. Decisions concerning up-front classification practices (such as portion marking, which designates the parts of a record that are classified and the degree of protection needed) often proceed without any real consideration for how these practices will affect subsequent use of the records or efforts to declassify them. In fact, the tremendous backlog of records currently being encountered in the systematic review of older documents, discussed in Chapter III, is in large part the result of poor records management practices at earlier stages of the records' life cycle. Despite recent initiatives being developed by the National Archives, the Federal Government as a whole still lacks any coordinated plan to oversee the creation and management of electronic records, which encompass a rapidly growing share of the documents and images now being created and classified.

> Despite being required to mark documents to indicate which portions are classified and which are not, employees in some agencies continue to mark materials "Entire Text Classified," increasing the difficulty of distinguishing which parts truly need protection and which might later be declassified.

This life cycle approach recognizes that both classified and unclassified information (and the records in which that information is contained) exists throughout a life span in which decisions must be made with respect to creation, management and use, and final status (typically either destruction or preservation and release). Unlike other information, however, the management of classified information should include the important initial consideration of whether the information should be classified at all. Yet classifiers continue to consider the benefits of classification without giving equal weight to its costs, an unbalanced approach that has led to too much classification and weakened protection of the nation's core secrets. The life cycle approach thus incorporates the more general "risk management" approach to security which, as the Joint Security Commission (JSC) stated in 1994, includes an appraisal of "asset valuation, threat analysis, and vulnerability assessments . . . along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what countermeasures to apply."[5]

The "life cycle risk assessment" of classified information should encompass an analysis at each stage of the information's "life" of: (1) whether the information requires protection (given the risks, threats, and vulnerabilities to it) and, if so, how much and for how long; (2) the public's right to know about the functioning of government and whether this outweighs the need for protection in a given instance; and (3) the cost of protecting or declassifying the information. This approach also recognizes that consideration of these criteria may lead to different results at different stages of the life cycle. For example, the public benefit in knowing the information initially may be outweighed by the need for its protection, but later may carry greater relative weight and may require its release.

Success in institutionalizing such an approach at all stages in the management of classified information would result in significant benefits. These include helping to foster a better understanding and acceptance of why information was classified in the first place, enhancing the protection of information, and improving the efficiency with which resources devoted to information management are used, thus reducing costs.

The Secrecy System

Bases for Classification

A Half Century of Executive Orders

Executive Order 12958, like prior orders, lays out the rules governing the identification and protection of information, the unauthorized disclosure of which could cause "damage to the national security." The now-common practice of specifying categories of information eligible for classification began in 1978 when President Carter's Executive Order 12065 set out seven such categories, an approach seen at the time as a possible way to reduce initial classification actions. Examination of the Carter Order and subsequent orders, however, reveals only the slightest difference in the *kinds* of information eligible for classification under each. Two categories (confidential sources and cryptology) under President Reagan's Executive Order 12356 were combined with other categories under Executive Order 12958. The so-called "catch-all"

category that allowed agency heads to classify "other categories"of information was rarely invoked, and was deleted under Executive Order 12958.

> One official involved in drafting Executive Order 12958 acknowledged that anyone seeking to classify a piece of information not explicitly covered by the Order would have to be "unimaginative" not to be able to "fit" the information into one of the seven categories.

There has been no shortage of suggestions on how to reduce classification by restructuring the definitions of the categories of information eligible for classification. The Joint Security Commission, for example, proposed several "limited categories" of information that would qualify for its "Specially Protected" category. The review effort that led to Executive Order 12958 also considered narrowing existing definitions, but the interagency group charged with drafting the Order was unable to reach consensus on how to narrow the criteria. Although the categories as provided in Executive Order 12958 could be more narrowly drawn, at the same time they must be broad enough to allow different departments and agencies latitude to interpret them according to their diverse needs. The Commission cautions, however, against viewing changing the scope of these categories as a "silver bullet" that alone will reduce unnecessary classification.

Despite the difficulties inherent in trying to adjust classification criteria, a different approach—one based on the need for genuine risk assessment—can complement the more deliberative process of classification decisionmaking and focus classification on the core secrets that must remain protected. The categories of information eligible for classification should be narrowly defined, allowing exemptions only in specific, carefully-defined instances requiring approval by the National Security Council (NSC). Under the statute proposed in Chapter I, the President would retain the authority to determine which categories of information should be open to classification.

Classification categories that should be considered are:

- Technical information on the design, development, vulnerability, capability, or use of weapons systems, cryptologic systems, and imagery.

- Names/identities of those individuals or organizations that provide information to the U.S. Government with the expectation that the information will be held in confidence or, if further disclosed, would pose a substantial risk of harm to the individual or organization that provided it.

- Foreign relations or foreign activities of the United States, that, if disclosed, would impair foreign policy.

- Plans for or conduct of military operations that, if disclosed, would impair the effectiveness of present or future operations or jeopardize human life.

- Sources and methods used to collect, process, and analyze information included under the traditional disciplines of signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), and human-source intelligence (HUMINT).

- Foreign government information, the protection of which is specified by the terms of a treaty, agreement, or other international obligation.

What distinguishes some of the above categories from past proposals and the current executive order is that, for the first time, they include *thresholds* for classification. For example, in past executive orders, any information concerning the "foreign relations and foreign activities of the United States" could be considered for classification. Under this suggested approach, such information would still be eligible for classification, but only if it would *impair* those "relations" or "activities," requiring classifiers to make a reasoned evaluation of whether the information truly warrants classification. While the Commission recognizes that those determined to classify information will not allow definitional hurdles to stand in their way, the proposed approach at least should prompt classifiers to think more carefully before doing so, resulting in more reasoned decisions and, perhaps, less classification.

Protection of Sources and Methods

The National Security Act of 1947 tasks the Director of Central Intelligence (DCI) to "protect intelligence sources and methods from unauthorized disclosure." Since 1978, executive orders have specifically authorized the classification of sources and methods information. While charging the DCI with a statutory obligation to protect "sources and methods" may seem redundant, the extensive classification system of today did not exist when the Act was passed half a century ago; the first government-wide executive order on classification came four years later. Classification thus has been the tool by which the DCI (and by extension the intelligence agencies under his authority) has met this statutory obligation.

However, neither the National Security Act nor any of the relevant executive orders has defined what constitutes a "source" or a "method," and the use of these provisions has been the subject of frequent criticism. Protection of sources and methods has been used to justify the classification of a range of information sometimes only indirectly related to a specific source or method. Sometimes included in this are "open sources" such as books, newspapers, and public broadcasts, which can in some areas (such as economic analysis) account for up to 95 percent of the information collected by the Intelligence Community.[6] The view that even such open sources can reveal the methods by which analysts process information and reach their conclusions has also affected agencies' responses to public requests for information, as discussed in Chapter III.

Protection Under the Atomic Energy Act

The Atomic Energy Act of 1954 (AEA), as amended, authorizes an entirely separate system for protecting information from that established by executive order. This distinct system arose from the desire to establish a special regime for protecting highly sensitive nuclear-related information, coupled with the absence of any formal classification system among civilian agencies immediately after World War II. The AEA serves as the basis for between 80 and 90 percent of all classification decisions made by the Department of Energy (DoE), according to Department officials.

The AEA provides for the classification of information, termed Restricted Data (RD), covering "the design, manufacture or utilization of atomic weapons . . . the production

of special nuclear materials . . . or the use of special nuclear material in the production of energy." Unlike national security information, which must meet certain criteria before being classified, no affirmative decision is required on the part of the DoE to classify information as Restricted Data: if information fits within the above definition, then it is considered classified from its origin and is said to be "born classified." Statutory authority for the classification of such information also has implications for oversight of DoE classification practices, as discussed below.

While authority for declassifying Restricted Data lies solely with the DoE, the approval of the Department of Defense is required when moving out of the RD category ("transclassifying") information that "relates primarily to the military utilization of atomic weapons." Although not specified as such in the AEA, this transclassified information is referred to as Formerly Restricted Data (FRD). In almost every respect (with the exception that it cannot be shared with another country absent an agreement authorized under the AEA), FRD is treated and handled in the same way as national security information classified under executive order. Like national security information, RD and FRD can be classified Confidential, Secret, or Top Secret.

The separate statutory basis for protecting nuclear information also has affected the process for declassifying this information. This process has been criticized as burdensome, inflexible, and costly by many scientists, environmental researchers, and other scholars. These critics contend that the system for declassifying RD fails to take into account scientific and technological changes, to allow reasonable access to information about environmental hazards caused by nuclear-related activities, or to consider the voluminous information now in the public domain on atomic energy and related matters.[7] The DoE's comprehensive, agency-wide effort to increase public confidence through a policy of greater openness has aided progress toward decreasing the amount of information remaining classified. Its Fundamental Classification Review (discussed further below) used a panel of leading nuclear scientists, historians, and agency representatives to reevaluate the extent to which information now classified as RD or FRD can be made publicly available. Attention to these matters should continue through the DoE's Openness Advisory Committee, composed of distinguished professionals who are responsible for advising the DoE on issues related to declassification and openness.

Since 1992, three studies—all commissioned by the DoE itself—and the draft of the still-pending Fundamental Review have called for eliminating the FRD category, asserting that information within it can be adequately protected by either the traditional classification system or the RD category.[8] One of these studies, issued in 1995 by a National Academy of Sciences task force, explicitly encouraged this Commission to consider "whether there is any continuing justification for two separate and parallel classification systems."[9] The Commission concludes that, as long as RD and FRD are controlled by a separate statute, legislative action will be required to bring meaningful changes to the DoE's current classification system and to bring it into greater harmony with the overall system for controlling access to national security information.

Living With Ambiguity: The Levels of Classification

Individuals who have already decided to classify a piece of information then must decide on the level at which to do so. Executive Order 12958 preserves the three classification levels of Confidential, Secret, and Top Secret that have long served as the foundation for protecting classified information. While elements of the definitions of these three levels have varied over time—Executive Order 12958, for instance, is the first to require classifiers to be able to "identify and describe" the damage to the national security if the information were disclosed—they have remained based on the concept of "damage" since the 1950s. If the unauthorized disclosure of the information could potentially cause damage, it may be classified Confidential; Secret if "serious damage;" or Top Secret if "exceptionally grave damage." Most classifiers employ the middle option: 71 percent of all classified information is Secret; only 20 percent and 9 percent of all classified information is Confidential and Top Secret, respectively.[10]

> The three classification levels are commonly referred to as the "collateral" system—a term meaning "ancillary"—a revealing point, since these three levels are intended to be the core of the classification system.

The difficult task of differentiating between such vague standards has long been criticized by many classifiers, recognizing that reasonable people may well disagree over the degree of damage certain information might cause if disclosed and, thus, over the level at which it should be classified (as well as whether it should be classified at all). This subjectivity has been one of the major factors leading to calls for reducing or consolidating these levels.[11] Most recently, the Joint Security Commission recommended the creation of a "one-level classification system" in which, according to the JSC, the only difference between information with the potential to cause different degrees of damage would have been the type of physical protection it received. Yet even under the JSC's "one-level" proposal, classifiers still would have been required to select and apply one of two "degrees of [physical] protection." In addition, although changing the number of levels may simplify the classification system, the Commission has found no evidence that such a change would reduce the amount of classification.

Controlling Access to Secrets: The "Need-to-Know" Principle

The granting of a security clearance for a certain level of classified information is not supposed to mean that an individual gains *access* to all information classified at that level. The dissemination of classified information is intended to be limited to those who both (1) hold the appropriate clearance, and (2) need the information in order to properly perform their duties. The extent to which the "need-to-know" principle is adhered to in practice, however, has been the subject of debate and disagreement for decades.[12] The placing of classified information on automated information systems presents additional challenges in this regard, as a growing number of cleared personnel are able to access classified information for which they may not have a genuine need. Intelink—the Intelligence Community's version of the Internet, which allows cleared personnel access to a range of classified information—provides one notable example of how need-to-know is becoming harder to enforce in the Information Age.

The difficulty of discerning who truly needs access to classified information has contributed to the rise of a host of methods for limiting such access. A variety of control markings and handling caveats restricts the dissemination of information and has added extra layers to the classification system. For example, thirteen access

categories (known as Sigmas) limit access to Restricted Data, and within the Intelligence Community the control marking "ORCON" (Dissemination and Extraction of Information Controlled by Originator) prohibits further dissemination without the specific approval of the originator of the information.

Clarifying Security in Special Access Programs

Access to information considered to be particularly sensitive is controlled through a range of special access programs, which involve access controls and security measures typically in excess of those normally required for access to classified information. (Unless specified as Department of Defense (DoD) Special Access Programs (SAPs), the term "special access program" is used throughout this report to denote any program that limits access beyond that of the three-tiered collateral classification system.) These include programs within the Departments of Defense, Energy, and State, as well as the plethora of compartments within the Intelligence Community designed to protect intelligence information and material referred to as Sensitive Compartmented Information (SCI). The legal basis for creating such programs flows from successive executive orders and, in the case of SCI, from the National Security Act of 1947 and Executive Order 12333 (which lays out the responsibilities of various intelligence agencies). Other special access programs, such as those relating to the protection of the President, the continuity of government operations, and covert action (all known as "national programs"), are operated from within the Executive Office of the President.

A Special Access Program

The Congressional Emergency Relocation Site (located under the Greenbriar Hotel in West Virginia and built to house the entire Congress and some of their staff in the event of a national security emergency) was designed, constructed, and maintained as a special access program for more than thirty years until 1994 when its existence was declassified.

Additional security requirements to protect these special access programs can range from mere upgrades of the collateral system's requirements (such as rosters specifying who is to have access to the information) to entire facilities being equipped with added physical security measures or elaborate and expensive cover, concealment, deception, and operational security plans. Such measures often have been justified as the only way to provide the security necessary to protect information considered especially sensitive. Programs can concern research, development, and acquisition activities; intelligence; or military operations. They can be funded by one agency but managed by another, which often leads to difficulty in simply accounting for how many programs exist and how much money is spent on them.

Publicly acknowledged programs are considered distinct from unacknowledged programs, with the latter colloquially referred to as "black" programs because their very existence and purpose are classified. Among black programs, further distinction is made for "waived" programs, considered to be so sensitive that they are exempt from standard reporting requirements to the Congress. The chairperson, ranking member, and, on occasion, other members and staff of relevant Congressional committees are notified only orally of the existence of these programs.

There are approximately 150 DoD-approved SAPs (the exact number is classified and others have been created but not yet formally approved), down from 200 in the late 1980s, and roughly 300 SCI compartments, compared with an estimated 800 in the late 1980s.[13] These numbers, however, do not include the many subcompartments, perhaps best termed "SAPs within SAPs," that further limit the extent to which personnel have access to various parts of the same program.

A notable example of the declining use of such programs to protect information considered especially sensitive is the reevaluation of how to best protect certain imagery capabilities (which also led to the declassification of large amounts of imagery dating from the 1950s and 1960s). Since 1995, an estimated 95 percent of all imagery derived from electro-optical image systems and once restricted to a highly classified SCI compartment has been produced and disseminated at the Secret level. As a result, this information can now be more widely disseminated to government "consumers," such as the military, which has relatively few individuals cleared above the Secret level.

In 1994, the DoD created the Special Access Program Oversight Committee (SAPOC) to standardize and formalize the approval, termination, revalidation, and restructuring procedures for DoD special access programs. As required by Executive Order 12958, the SAPOC annually reviews and validates all previously identified DoD special access programs for continued special access program status. The review process is intended to validate the need for continued security compartmentation or to restructure a program into either another special access program or a "collateral" program, and seeks to eliminate redundancy among programs. The SAPOC is intended to provide senior leadership, oversight, and management of all DoD special access programs, to ensure compliance with applicable executive orders and other policies and procedures, and to ensure that required information is provided to the Congress. Within the Intelligence Community, the Controlled Access Program Oversight Committee (CAPOC) performs much the same function as the SAPOC, including annual review of all such programs as required by Executive Order 12958 and a report to the Congress. The CAPOC includes within its review the SCI control system compartments and special access programs funded by the National Foreign Intelligence Program.

> Many of the industrial contractor representatives who attended Commission Roundtables noted that there appear to be unlimited budgets for security in many special access programs and a failure to weigh the value of additional security against its costs.

However, while carefully assessing program cost, schedule, and performance, these reviews have not always focused on the special security features imposed and their associated costs. Despite the improvements described above, concerns have been raised that the SAPOC is too senior a body to have the necessary working knowledge and expertise to adequately address the security procedures and costs associated with DoD special access programs.

More generally, the lack of standardized security procedures for special access programs contributes to high costs and other difficulties. The Joint Security Commission (JSC) recommended a "single, consolidated policy and set of security standards" for such programs, but nearly three years later this recommendation has not been implemented.

Industrial contractors performing classified contracts are governed by the National Industrial Security Program (NISP), created in 1993 by Executive Order 12829 to "serve as a single, integrated, cohesive industrial security program to protect classified information." A Supplement to the NISP operating manual (NISPOM) was issued in February 1995 with a "menu of options" from which government program managers can select when establishing standards for contractors involved with special access programs. However, industrial contractors report that wide variations still exist in the standards applied by government program managers of different SAPs. The "menu of options" continues to allow conflicting and costly security requirements. For example, a senior security officer from a large industrial contractor presented the Commission with a thick set of supplemental forms—all prepared by different program managers and often requesting the same information—that frequently are required before contractor employees can be granted access to certain special access programs.

Within the Intelligence Community, special access programs have been standardized by DCI directives, while those within the DoD continue to operate based on a menu with a wide variety of choices. Some military services continue to increase security regulations for SAPs, while others try to do the opposite. To address this problem, many industry representatives suggest establishing a clearer "baseline" standard and then requiring a specific justification before any additional security can be imposed.

Recommendation

The Commission recommends that the Security Policy Board (SPB) implement within one year the JSC recommendation on establishing a single set of security standards for SAPs. The SPB, in conjunction with the DoD, should examine whether the NISPOM Supplement should continue to allow individual SAP program managers to select the security measures for their program rather than conform to a single standard. Industrial contractors should be included in this review and in the development of a single set of standards.

Protecting Other Government Information

It is impossible to understand how the classification system regulates classified information without taking a broader look at the entire process of protecting all government information. Although by definition not part of the classification system, unclassified information viewed by government agencies as needing protection has implications for the amount of information that is classified. Though sensitive information has never been addressed by executive order, the Computer Security Act of 1987 defines it as "information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs." Responses to a Commission questionnaire revealed at least 52 different protective markings being used on unclassified information, approximately 40 of which are used by departments and agencies that also classify information.[14] Included among these are widely-used

markings such as "Sensitive But Unclassified," "Limited Official Use," "Official Use Only," and "For Official Use Only."

Agencies protect some unclassified information in response to legal mandates (such as the Privacy Act) or specific agency regulations. Most specify the types of information that fall into this category, ranging from the very broad and general (e.g., "adverse effect upon the national interest" if disclosed) to the very detailed and specific (e.g., particular aspects of atomic energy defense programs). Agencies control access to this information through a need-to-know process, store it in locked desks or cabinets, and provide at least rudimentary protection when used in automated information systems. Still, there is little oversight of which information is designated as sensitive, and virtually any agency employee can decide which information is to be so regulated.

Moreover, the very lack of consistency from one agency to another contributes to confusion about why this information is to be protected and how it is to be handled. These designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information. Numerous officials expressed concern to the Commission about the protection and handling of their agencies' information by other agencies; some even admitted to classifying information inappropriately to ensure its protection. A related concern arises from U.S. compliance with agreements under which it is obligated to protect information provided by foreign governments at a level at least equal to that provided by those governments. Lacking any clear level of protection for unclassified sensitive information, the U.S. Government must protect a great deal of unclassified foreign information as though it were classified, thus incurring the accompanying security costs.[15]

> Some officials admit to classifying information that should not be classified so that it would fall under the more clearly defined boundaries of the classification system and receive greater protection.

In 1986, the Government attempted to address concerns that easy access to multiple databases made it increasingly likely that adversaries could piece together highly sensitive technical information from unclassified sources by proposing creation of a new category of sensitive but unclassified information. However, the resulting outcry over the specter of government control of information in commercial databases caused the proposal to be quickly dropped, but not before the term "sensitive but unclassified" came to be associated by many with unwarranted government attempts to control unclassified information. Over a decade later, the Commission finds that the problems associated with ensuring both the protection and public availability of sensitive information continue to complicate the efficient administration of the classification system and believes that the Executive Branch should examine more thoroughly whether resolution of this problem is possible.

The Classifiers

Original Classification Authorities: The Linchpin of Classification

Under Executive Order 12958, Original Classification Authorities (OCAs) are defined as the only individuals permitted to "classify information in the first instance." Typically

department or agency heads, or other senior government officials, OCAs are designated in writing by the President.

In response to studies that identified the number of original classifiers as a contributing factor to the amount of classification and noted that many individuals possessed the ability to classify originally simply because it was viewed as a measure of status**,** many agencies have dramatically reduced the number of people with that authority.[16] As of 1995, there were fewer than 5,400 individuals specifically authorized to classify information in the first instance, the smallest number since such statistics were first collected in the early 1970s (when almost 60,000 persons had that authority).[17]

While OCAs account for only six percent of all classification actions in any given year, this does not provide an accurate measure of their influence on the overall amount of information classified. As the only individuals actually designating what information is classified, their decision to classify particular information constitutes the first stage of its life cycle as national security information. Many original classifiers also are responsible for the classification guides that others use in the course of their daily work. A decision to include a piece of information in such a guide thus can lead to a multitude of subsequent "derivative" classification actions.

Until recently, very little was required of any classifier when making a classification decision. Executive Order 12958 for the first time requires OCAs to justify their decisions by completing a classified "why line," in which they must explain why the information warrants classification (a requirement that can be satisfied by citing a relevant category of classifiable information). In addition, the Order requires original classifiers to identify themselves on the materials they classify. Added attention to proper classification should also come as a result of the Order's requirement that "management of classified information" be included as "a critical element or item to be evaluated in the rating" of original classifiers.

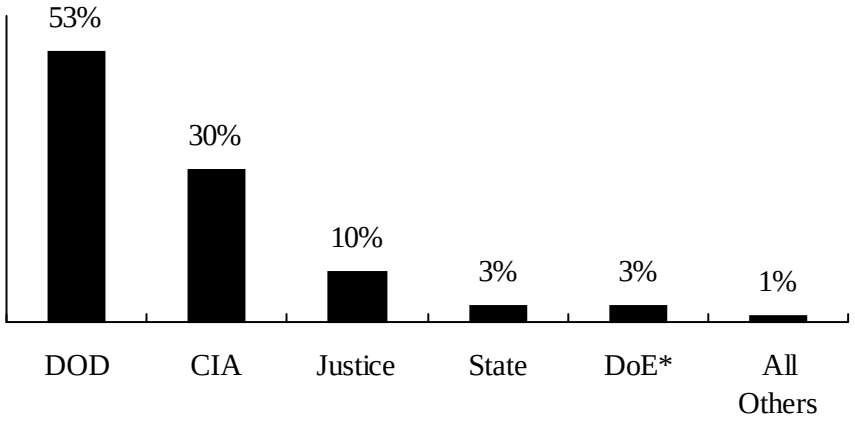
> A single decision by an OCA to include a piece of information, data, or technology in a classification guide can lead to thousands of subsequent "derivative" classification actions.

Because the original classification decision is the linchpin on which all other subsequent decisions depend, extreme care should be taken in making this initial decision. The current practice of merely citing one of the categories of classifiable information on the "classified why" line does little to lessen the tendency to classify by rote and does not adequately reflect the long-term consequences of an original classification decision. Requiring all original classifiers to provide a more detailed justification for each original classification decision would assist in this regard. Such a statement could include: (1) the damage to the national security that might result from the unauthorized disclosure of the information, as well as the other criteria (discussed below) used in making the decision; (2) how the information differs from information already classified; and (3) the classification guidance consulted in determining that the information was not already classified**.**

Both the Central Intelligence Agency (CIA) and the DoE already have such a requirement and report no significant administrative burden in its implementation; the DoE notes that it allows for enhanced oversight by permitting internal review of original decisions. Requiring such a written justification would prompt original classifiers to

think more carefully about their decisions and make a more concerted effort to consult existing classification guidance. A written record of original decisions might have the added benefit of encouraging the preparation or updating of classification guides. Finally, an explanation of the intent behind a decision should assist both in oversight of classification decisions and the life cycle management of information by helping others determine subsequently whether the information still warrants classification.

Figure 1:
Where It Happens: Classification By Agency



Source: Averages for all classification activity (original and derivative) for years 1990-1995 as reported by the Information Security Oversight Office.
*RD and FRD at the DoE; figures provided by the DoE.

Derivative Classifiers: Enhancing Accountability Where it Matters

Ninety-four percent of all classification actions in the last six years have occurred when personnel have classified "derivatively" by extracting or paraphrasing information in already-classified materials or by using their own interpretation of what they believe requires classification, including the use of classification guides.[18] Unlike original classifiers, those who classify derivatively are almost never designated in writing (the DoE being an exception). Virtually anyone with a security clearance, from the entry-level soldier to an employee of an industrial contractor to a political appointee, can classify information derivatively; the CIA and the National Security Agency (NSA) are but two examples of agencies where nearly all employees are potential derivative classifiers. While over 80 percent of all classification occurs within the DoD and the CIA alone (Figure 1), an estimated three million government and industry employees today have the ability to mark information as classified.[19]

> An estimated three million government and industry employees today have the potential ability to mark information as classified.

Many of the individuals who classify derivatively remain unfamiliar with the proper procedures and even are unaware that it is something in which they are engaged, raising fundamental questions about the accountability, oversight, and training of those

making the majority of all classification actions. When there is little chance anyone will be able to determine the source of a classification action and hold the classifier accountable for it, the derivative classifier has little reason to think seriously about whether classification is really justified.

Requiring the identification of derivative classifiers could help begin to change this mindset. Some agencies—such as the CIA, DoE, National Reconnaissance Office (NRO), and Treasury Department—already require that all personnel identify themselves on the documents they classify, and they report few administrative problems. A separate line for classification would distinguish responsibility for classification from responsibility for content, assist with agency oversight of classification management and classification challenges, and help with processing Freedom of Information Act (FOIA) requests. Furthermore, knowing that they would be associated with the classification of a document over its life cycle, derivative classifiers might become more likely to consult classification guides**,** seek guidance from superiors, and properly portion mark documents—in short, to weigh the classification decision more carefully.

In contrast to Original Classification Authorities, most derivative classifiers are not required to be evaluated on their classification actions. Although Executive Order 12958 states that such performance ratings should be given to those "whose duties significantly involve the creation or handling of classified information," most agencies have not applied this requirement to those who classify derivatively. As a corollary to improved training for derivative classifiers (recommended below), long-term benefits could accrue by including the proper classification of information (the classification of only that information required for the legitimate protection of national security) as a critical element in the performance evaluations of *all* those authorized to classify. Knowing that one will be evaluated based, in part, on careful attention to classification responsibilities would provide a positive incentive to exercise this duty responsibly.

Developing Better Classification Guides

That so many government and industry employees are engaged in classification raises numerous issues with respect to the guides used by derivative classifiers—guides which equate to a delegation of classification authority.[20] The quality of guides can have an enormous impact on the quality of the entire classification system; approximately 94 percent of all classification decisions are based on these guides, or on other previously classified material. There are thousands of classification guides throughout the Government, many of them hundreds of pages long, and many themselves classified. The vast majority are found within the DoD, which reports over 2,000 guides, most covering weapons systems.

With different agencies (and different programs within agencies) preparing guides, they can sometimes contradict one another. Another problem is the failure of some agencies to regularly update these guides, a matter of particular concern to industrial contractors who must rely on guides often prepared without their input and which, at times, fail to consider information already in the public domain. As required by Executive Order 12958, many agencies now are reviewing and updating their classification guides, a development that may improve the quality of these guides.

Those who classify must have a clear understanding of how their senior managers view classification management and how they want them to approach their classification responsibilities. Some agencies attribute a decrease in original classification decisions to the increased use of classification guides. For the successful implementation of a life cycle approach to information management, and given the exponential effect of guides on subsequent derivative decisions, it is imperative that guides be reviewed frequently. Equally critical is that these reviews include a risk assessment analysis to determine whether information still requires the same level of protection or whether protection is still needed at all. Those guides pertaining to industrial programs could benefit from the input of contractors. More up-to-date guides should also assist with the declassification of information, as discussed in Chapter III.

Improving the Training and Education of Classifiers

The subjective nature of classification decisions accentuates the need for effective training and education to ensure that classification is employed only when truly necessary. Yet the vast majority of derivative classifiers receive little, if any, formal training, and OCAs often are able to avoid training altogether. Although numerous executive orders have called for general security training, none has required agencies to ensure that derivative classifiers receive initial training or remain proficient in classification throughout their careers. Declining budgets have further limited the ability of agencies to provide training programs, which tend to be both resource and personnel intensive.

Executive Order 12958's requirement that original classifiers "receive training in original classification" constitutes an important step in attempting to improve the quality of classification decisions. However, while offering suggestions as to what agencies *might* include in this training, neither the Order nor its implementing directive establishes minimum standards for this training, and there are no current plans to consider such minimum standards. Moreover, no training is required for derivative classifiers. To their credit, several agencies maintain formal training programs for those authorized to classify, although these vary widely and the number of personnel involved remains small.

Emphasizing Training

The Headquarters Army Materiel Command in June 1996 mandated that its 800 personnel (all but two of whom were derivative classifiers) attend a series of briefings on Executive Order 12958.

Quality training can play a significant role in developing more proficient classifiers and better life cycle management of government information. As the ISOO has recognized, training would "reduce the volume of information unnecessarily classified by improving the competence . . . of classifiers" and would "increase uniformity in the application of classification principles and marking."[21] Information can be better protected when classifiers understand what they are protecting and why. Initial training would ensure that classifiers have the basic tools to perform their duties, and ongoing education would reinforce that training. Internal computer services such as the NSA's "Policy On Line," which encourages the two-way flow of information between agency personnel and classification management specialists, offer one way to provide enhanced employee awareness of and proficiency in classification practices.

Expanding the training mandated in Executive Order 12958 for original classifiers to include derivative classifiers, and requiring periodic attendance at agency programs on

classification designed to ensure continued proficiency over time, are but two ways to improve the practices of classifiers. Training, subject to minimum Executive Branch standards, could also serve as a prerequisite for being evaluated on one's approach to classification, as suggested below.

Recommendation

The Commission recommends that agencies take several steps to enhance the proficiency of classifiers and improve their accountability by requiring additional information on the rationale for classification, by improving classification guidance, and by strengthening training and evaluation programs.

Elements of this approach should include:

- Original classifiers shall provide a detailed justification for each original classification decision;
- Derivative classifiers shall be required to identify themselves on the documents they classify;
- Classification guides shall be better developed, more definitive, and updated regularly, and industry shall participate in the preparation of guides affecting industrial programs;
- Training shall be expanded to include derivative classifiers and shall conform to minimum Executive Branch standards; and
- Proper classification of information shall be included as a critical element in the performance evaluations of *all* employees authorized to classify.

The Key to Better Classification: The Initial Decision to Classify

The Importance of the Initial Decision

As a result of the system described above, classifiers must engage in a two-step process of first determining whether the information qualifies as one of the categories of information eligible for classification, and then whether its unauthorized disclosure could reasonably cause damage to the national security. In reality, however, these two steps often are compressed into one, in which all information falling into the eligible categories is classified. In part, this is a reflection of Executive Order 12356, which for over a decade directed that such information "*shall* be classified" (emphasis added). Yet under Executive Order 12958, simply because information *could* cause damage does not mean it *must* be classified; the new Order makes it clear that information falling into one of the categories of classifiable information *may* be classified,

and that "if there is significant doubt about the need to classify information, it shall not be classified."

The task of deciding which information is to be classified, at which level, and for how long remains in large part a subjective judgment open to a range of interpretation. The absence of widespread training and the unavailability or lack of clarity of some classification guides only make appropriate classification decisions all the more difficult. Experts in classification management have pointed out that this first step of the classification management process—the identification by original classifiers of information that should be protected, coupled with derivative classifiers' interpretation of those decisions—tends to be the weakest link in the process of identifying, marking, and then protecting the information.

To reduce this subjectivity, several agencies are developing or already using technologies that attempt to quantify the damage that information might cause if disclosed and then actually make decisions for the classifier. However, even the most advanced programs cannot reduce entirely the subjectivity inherent in classification. Of potentially much greater benefit are "decision tools" that can assist classifiers in making classification decisions. These tools, such as one being developed at the NRO, guide classifiers through the process step-by-step, permitting a computer-generated document to be classified only after the preparer has gone through all the necessary steps and certified that the information contained within the document satisfies the criteria for classification. The National Security Council has taken this approach one step further, applying it to electronic mail; "masks" prevent NSC personnel from sending or printing internal electronic mail messages until they have certified whether classification is needed, a reform that, according to one former official, has contributed to a recent decrease in the amount of classification at the NSC.[22]

The importance of the initial decision to classify cannot be overstated. Classification means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to information that would be unnecessary if the information were not classified. Classification also means that those who need the information in the course of their work have to be investigated and adjudicated for access. Classification further means that a document may have to be edited to remove some of the most sensitive details if it becomes necessary for the information to be more widely distributed. Finally, classification means that some form of review will have to take place if and when the document is considered for declassification, archiving, or long-term storage.

> One official involved with the drafting of Executive Order 12958 expects it to "do little" to reduce the amount of information that is classified.

All too often, however, attention has focused on other aspects of the classification process, such as the level at which the information is to be protected after it is classified. The JSC's call for a "one-level classification system" was only the most recent in a long line of proposals to restructure the levels of classification or overhaul the entire three-tier classification structure. Yet even the JSC made clear that its proposal was designed primarily to streamline the system and reduce costs, and not to reduce the amount of information classified at the outset (although it argued that this could be a by-product of a less complicated system).[23] In addition, key officials involved in the development of Executive Order 12958 have acknowledged that the Order focuses more on

the declassification of already classified information than on policies that would reduce the amount of information classified at the outset.

Despite the significance of this initial decision, relatively little is known about exactly how much information is classified. Much of this uncertainty derives from the fact that over two decades of statistical reporting by the ISOO and its predecessor, the Interagency Classification Review Committee, have chronicled classification "actions" (the individual act of designating a document as classified by either an original or derivative classifier) rather than the actual amount of classified materials generated. These actions are based on extrapolations of samplings that often take place at different times and vary in duration from agency to agency. The more than 3.5 million actions reported in 1995 are an extremely rough estimate of the number of actions that may have occurred that year. Nor does this estimate necessarily correlate to the number of pages, computer diskettes, or images classified that year, since a single action can result in the classification of a one-page memorandum or a document hundreds of pages long.

Given this uncertainty, it should not be surprising that there is little agreement on the extent of *over*classification. For over a decade the ISOO has estimated that between one and ten percent of all classified documents are unnecessarily classified.[24] In 1995, a White Paper prepared by the DoD Inspector General concluded that the classification process at the DoD is "fundamentally sound" and that "the present size of classified holdings is not the result of too much information being needlessly classified."[25] In contrast, a 1985 preliminary study prepared by the staff of two House subcommittees proposed a classification system in which "roughly nine-tenths of what is now classified" would no longer qualify for classification.[26] More recently, former NSC Executive Secretary Rodney B. McDaniel estimated that only ten percent of classification was for "legitimate protection of secrets."[27] Given the uncertainty surrounding the breadth of classification, however, efforts to quantify with any precision the extent of unnecessary classification not only may be futile, but are unlikely to help in understanding its causes or possible remedies.

It may be more meaningful to recognize that the perennial problem of unwarranted classification attests to the continued failure of classifiers to engage in a rigorous assessment of the need for classification. For instance, in seeking to protect information about certain weapons systems (the classification of which has been permitted under successive executive orders), many of the support functions associated with these systems, such as information concerning logistical and administrative support, have also been classified even though it was doubtful that their disclosure could have caused any damage to the national security. In the Commission's review of one intelligence agency's documents, a memorandum to employees of the agency describing an upcoming "family day" in which family members could visit the agency was classified Confidential because the person who signed the memorandum was under cover. By simply omitting the name of that individual, the memo would have been unclassified. The entire agenda for a Commission meeting at one intelligence agency was classified because one word—not crucial to the topic being discussed—revealed a classified relationship. At other meetings, Commission staff inquiries as to why certain briefing slides were classified were met with responses such as "I'm not sure," or "This is just the way we prepare our materials."

Improving the Initial Decision

To the credit of many officials, there has been a growing recognition of the need to replace a risk avoidance approach to security, which seeks to anticipate *all* risks in the protection of assets, with a risk management approach, which seeks to concentrate limited resources on those assets the loss of which would have the most profound effect on the national security. This perspective was reflected in the Joint Security Commission's conclusion that security managers "must make tradeoffs during the decision phase between cost and risk, balancing the cost in dollars, manpower, and decreased flow of needed information against possible asset compromise or loss." Some agencies have taken the initiative to go beyond what is required of them and have reevaluated the extent to which they employ classification. For example, the Department of Energy recently engaged in a thirteen-month Fundamental Review of its classification policies, its first such review ever, and in its draft report recommends that a number of topical areas no longer be classified.

These exceptions aside, three years after the JSC report, risk management continues to be more of a goal than an operative philosophy guiding today's security decisions. The desire to avoid any and all possible loss too frequently continues to be the predominant approach to security in general and to classification management in particular. However, the JSC's proposal to apply risk management to the classification system by restructuring that system entirely is only one way to reform the system. Concentrating on the initial decision of whether or not to classify—the point at which classifiers decide whether to place the information in that three-tiered classification structure—holds greater potential for improving the classification process and reducing the amount of information classified than does restructuring the entire system.

Costs vs. Benefits

The Navy requires that "the advantages and disadvantages of classifying . . . be weighed." Among the factors the Navy encourages its classifiers to consider are: cost, the "net national advantage" (to include the benefits of not classifying), and the ability of other nations to know or possibly to learn about the information.

Neither of the two steps for deciding whether or not to classify serves as a significant deterrent to unnecessary classification. Moreover, the emphasis on damage to the national security can contribute to unnecessary secrecy. Although some agencies, such as the Department of the Navy (see box), have gone beyond these criteria, the vast majority of classifiers still employ an approach that fails to reflect the magnitude of the decision to classify. Classifiers, instead, should consider a range of factors when making the decision to classify and, in so doing, undertake a more balanced analysis of whether classification is necessary. In this regard, the Commission seeks to build on the 1995 report of the National Research Council which, in its review of the classification and declassification practices of the DoE, recommended that before such decisions are made, "the benefits of classification [must] clearly outweigh the costs."[28]

The consideration of additional factors during the classification decision could reduce or eliminate the need for classification in a given instance. These could include the following factors:

- actual intention and ability of an adversary to inflict damage (threat);
- ability to defend assets in the event of an attack (vulnerability);

- probability of loss given threat and vulnerability (risk);
- resources required to avoid or minimize risk (cost);
- interest of adversaries in obtaining this information (value of information); and
- expected benefit of the information being publicly available (public release).

Such factors could be considered when original classification decisions are made, during the preparation of classification guides, and when derivative classifiers find themselves in situations where guidance is unclear.

Considering these factors could lead an official to conclude that while information may fall within one of the specified categories eligible for classification and might cause damage to the national security if disclosed, the actual threat to that information or likelihood of compromise may be so low or nonexistent that classification is not necessary. The costs of protecting a particular piece of information may be so high that they outweigh the possible advantages to be gained from its protection. In other cases, the sensitivity of information, or its value to the national security, may be so great that protection—no matter the cost—would be warranted.

Introducing these additional factors into the classification decisionmaking process may, in some cases, make this initial decision somewhat more difficult. However, given the long-term implications of the initial decision, a more deliberative process is necessary. This should allow for a more efficient use of classification in the short-term and lead to savings in both time and resources in subsequent reviews for downgrading or declassification.

The consideration of additional factors should not be viewed as an invitation to embark on intensive efforts to quantify these factors into complicated mathematical formulas or intricate computer programs. Patterned after the National Research Council's call for costs and benefits of secrecy at the DoE to be considered in their "broadest sense," the Commission believes that simply having to *think more* about whether classification is necessary may cause classifiers to give their decisions greater care—a process that should lead to more reasoned classification and may, in many cases, lead to less classification.[29]

Recommendation

The Commission recommends that classification decisions, including the establishment of special access programs, no longer be based solely on damage to the national security. Additional factors, such as the cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release, could also be considered when making classification decisions.

Enhancing Implementation and Oversight

Ultimately, a policy is only as good as its implementation. The fact that classification decisions will remain subjective judgments makes the need for meaningful oversight of implementation all the more critical. Yet responsibility for ensuring judicious classification today rests almost entirely within individual agencies, which rarely view reducing classification as a priority. Improved oversight requires renewed attention at three levels: the Congress, the Executive Branch as a whole, and the departments and agencies themselves.

A Greater Role for the Congress

Congressional oversight of how agencies implement classification policies pursuant to executive order has been virtually nonexistent. The Congress periodically has considered what the classification policies of the Executive Branch s*hould* be, but it has been far less active in reviewing whether the classification provisions of a given executive order are being implemented appropriately. Any congressional attention to how much classified information is generated has been mainly a by-product of hearings on how the failure to release already-classified documents has affected public access to information, as well as of recent efforts to focus on the costs of the system as a whole.

> Responsibility for ensuring meaningful classification today rests almost entirely within individual agencies, which rarely view reducing classification as a priority.

Greater congressional attention to agency classification and declassification practices would come through enactment of a statute, as recommended in Chapter I. Periodic oversight hearings would be an important start; holding senior agency officials accountable for their agency's classification practices would prompt greater attention to the long-standing problems described above. Furthermore, the Congress could use the confirmation hearings of senior officials to question them on their plans and approach concerning both access to and protection of government information. Of course, use of budget authority would be the ultimate leverage, and would offer a powerful incentive for senior agency officials to reduce the amount of information they classify, to protect more efficiently the information they do classify, and to make continued improvements to their overall information management programs.

The Focal Point: Executive Branch Policy Development and Oversight

Executive orders are the most visible element in the larger process of developing classification policies and then overseeing their implementation. However, confusion over the proper roles of the two organizations charged with policy development and oversight, the Security Policy Board (SPB) and the Information Security Oversight Office, combined with shortcomings in how each organization operates, have hampered the development and oversight of sound classification policies and practices.

Policy Development: Who's in Charge?

Responsibility for policy development lies primarily with the SPB, established within the National Security Council by Presidential Decision Directive (PDD) 29 in September 1994. The main impetus for creating such a body came from the Joint Security Commission, which found that the lack of a coherent framework for formulating,

implementing, and overseeing U.S. security policies was the "prime cause of the problems . . . associated with security policies, practices, and procedures." Emphasizing the need for "a unifying structure" capable "of pulling . . . disparate [government] elements together and overcoming bureaucracies' traditional resistance to innovation and change," the JSC called for a security executive committee to develop security policies across the Defense and Intelligence Communities and oversee their implementation. Because the JSC envisioned that this new body would also perform oversight, it noted that existing groups, such as the ISOO (tasked by executive orders since 1978 with conducting oversight of agencies' classification practices) could be consolidated under the new structure.

> Confusion over the proper roles of the SPB and the ISOO has hampered the development and oversight of sound classification policies and practices.

Although somewhat different from the body envisioned by the JSC in that it includes agencies outside the Defense and Intelligence Communities, the SPB is intended as the "principal mechanism" for the "coordination, formulation, evaluation and oversight of security policy."[30] Now composed of representatives from 35 agencies, the SPB is a multi-tiered structure of five permanent committees supported by a host of ad hoc steering committees and working groups; a Security Policy Forum composed of agency representatives at the Assistant Secretary level; and the senior-level Board itself, now co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence.

Under the SPB umbrella, many areas of security policy, such as personnel security, are coordinated more effectively than before. Representatives from various agencies now have a common venue to discuss matters of mutual concern. In contrast, however, responsibility for developing, implementing, and overseeing classification and declassification policies prescribed by executive order is not clearly defined, and is fragmented between the SPB and the ISOO. Less than a year after the SPB was created, Executive Order 12958 continued the practice of charging the ISOO with not only overseeing agency classification and declassification practices, but with leading "interagency meetings to discuss matters pertaining" to the Order—in other words, classification policy. In an effort to deal with this jurisdictional overlap, the ISOO Director serves as chair of the SPB's Classification Management Committee, a group which also serves as an advisory committee to the ISOO.

Officials of both the ISOO and the SPB acknowledge that this arrangement has been far from satisfactory and, on numerous occasions, has worked to the detriment of timely and coherent information security policy. For example, confusion over the roles of the two organizations resulted in some disagreement over the extent to which the SPB could influence the specifics of the directive implementing Executive Order 12958, a directive the President tasked to the ISOO. In addition, there was intense debate between the ISOO and the SPB staff over the degree to which agencies could "opt out" of certain provisions of the Order's safeguarding directive (laying out how agencies are to physically protect classified information), for which the SPB is responsible. Concerns raised by the ISOO were overruled, and member agencies moved to exempt themselves unilaterally from parts of the directive.

> Since its creation two years ago, the SPB has yet to issue a workable definition of risk management, failing to achieve agreement among the member agencies.

Nor are these problems restricted to the classification management arena. Significant problems remain with regard to the SPB's overall functioning. The SPB has failed to make meaningful progress on several key issues, such as developing an effective framework for applying (or even a workable definition of) risk management principles to security decisions, as well as implementing JSC recommendations to standardize the security rules applicable to special access programs. Despite this, several monthly meetings of the Security Policy Forum have been canceled because there reportedly were an insufficient number of agenda items or no substantive issues ready for decisionmaking.

Sound and coherent security policies have also suffered because the SPB process is premised on obtaining the agreement of all affected agencies through consensus policymaking, an approach explicitly criticized by the JSC. Member agencies have retained the ability to delay and dilute policies with which they disagree. Not only has this approach delayed progress, but it has meant that SPB products often go no further than the extent that the least supportive agencies will accept. As discussed in Chapter IV, although the SPB has produced adjudicative standards and investigative guidelines to improve clearance reciprocity between government agencies, these are only *minimum* standards; agencies may go beyond these standards, thus limiting the extent to which there is genuine reciprocity of clearances. And as of the printing of this report, the SPB had yet to produce the safeguarding directive cited above—nearly two years after being tasked to do so by the President. It seems reasonable to question whether this is what the JSC had in mind when it called for a group capable "of pulling . . . disparate elements together and overcoming bureaucracies' traditional resistance to innovation and change."

In addition, the SPB's plethora of committees and working groups has left the early crucial stages of policy development in the hands of less-senior representatives who may not even be aware of the positions advocated by the agencies' more senior officials. Indeed, these representatives have at times spent months negotiating consensus products, only to have these overturned by their own senior management at higher levels within the SPB structure. Moreover, the fact that the SPB staff, which also plays an influential role in policy development, is detailed from and will return to the very agencies affected by these policies is yet another example of how difficult it is for the SPB to represent anything more than the collective will of the government security bureaucracy.

With the exception of the access granted to the Commission staff, the SPB process remains largely isolated from outside observers. Because there is the potential that information of a classified nature may arise, meetings at all levels of the SPB structure are usually held in secure facilities, requiring attendees to possess security clearances. As a result, while certain industry group representatives with clearances have been permitted to attend meetings, other nongovernmental representatives without clearances cannot. Although a draft legal opinion by the Justice Department has affirmed this practice, the result is that policies developed within the SPB are debated and promulgated out of view of the public and of the Congress. All of this directly contradicts the JSC's vision of an organization that would "provide a focal point for Congressional and public inquiries regarding security policy or its applications."

Nor are the two entities that were designed explicitly to serve as venues for public input to the policymaking process actually doing so. In the same directive that established the SPB, the President (as the JSC recommended) created a five-member Security Policy Advisory Board to provide ongoing "non-governmental and public interest" input into the SPB process. More than two years later, however, only three positions have been filled, and there appears to be no active effort to fill the remaining two. Moreover, while these individuals carry impressive credentials, all come from government security and intelligence backgrounds. In addition, the Advisory Board deals only with issues referred to it by the SPB. Similarly, although an Information Security Policy Advisory Council (ISPAC) was created under Executive Order 12958 to "advise the President" on the policies contained in the Order, over a year and a half later none of the Council's seven seats have been filled, no meetings have been held, and none are expected for the foreseeable future.

Oversight: The Critical Missing Link

The SPB and the ISOO must also contend with overlapping mandates with respect to oversight. Although explicitly charged with oversight by Presidential Decision Directive 29, the SPB has devoted little or no time to such responsibilities. Yet even if it had done so, the value of such oversight would be questionable. Any such oversight would be conducted by the SPB staff, which lacks the resources to actively review agency practices and has little, if any, expertise on classification management issues. The unlikely prospect of the SPB staff aggressively reviewing the classification practices of their own agencies raises doubt about the independence and effectiveness of such oversight.

The potential consequences of the SPB's failure to pursue its oversight obligations, however, have been mitigated by the ISOO's continued activity in this area. As directed by Executive Order 12958, the ISOO continues to oversee agency classification practices. The ISOO has achieved some success, notwithstanding its limited resources and personnel and the fact that it has been shuffled among three different agencies in as many years.[31] Although questions have emerged concerning its ability to act independently of its new parent agency, the National Archives and Records Administration, the ISOO has remained independent of the agencies generating the bulk of classified information.

Nevertheless, Executive Branch oversight of classification practices has been and remains largely ineffective. In many respects, the ISOO has been reduced to a body that highlights ongoing agency practices rather than one that attempts to effect change in those practices. The height of the ISOO document reviews in the mid-1980s consisted of approximately one visit to each agency per year. The ISOO did not conduct a single on-site review of any agency's classified product for the two years between 1994 and late 1996. Moreover, despite its enhanced authority to oversee special access programs under Executive Order 12958, the ISOO has not yet done so. In addition, because the ISOO is limited to oversight of national security information, there is no

> The ISOO has achieved some success in the face of limited resources and personnel and being shuffled among three different agencies in as many years. Still, the ISOO has been reduced to a body that highlights ongoing agency practices rather than one able to effect change in those practices.

independent oversight of the 80 to 90 percent of DoE classification activity involving Restricted Data and Formerly Restricted Data under the Atomic Energy Act.

Given all of the above, it is not surprising that the ISOO's own Director has characterized its work as "overseeing agency oversight."[32] Yet the absence of more aggressive oversight by the ISOO may simply be an acknowledgment of its inability to enforce agency compliance with established rules. Although the ISOO has always possessed the authority to report on improper classification, acting on those reports remains the prerogative of the agencies themselves. In fact, while the ISOO often has been able to resolve disagreements by working with agencies, only once has it issued a formal report on abuse of classification to an agency.

Instead, the ISOO has directed much of its effort to describing agency classification practices in its annual report. This report has evolved significantly in recent years to include an array of statistical data on classification and declassification activity and, as of 1995, the costs associated with classification. Yet even this report, which is the ISOO's primary oversight tool, is widely considered within agencies to be more of an externally-imposed requirement than a helpful internal management tool—a point that has been confirmed by the ISOO Director himself. In addition, several agencies admit to doing little to ensure the accuracy of the data they report, further calling into question the value of these annual reports in their present form.

A New Approach to Policy Development and Oversight

Clearly, there needs to be a resolution of the respective roles of the SPB and the ISOO, as well as a strengthening of both policymaking and oversight functions in the classification management arena. Failure to do so risks compromising the quality of the policies themselves and their implementation at a time when institutionalizing sound information management policies is critical to the long-term credibility and success of the system for protecting the nation's secrets.

There are certain prerequisites if policymaking and oversight in this area are to succeed. With respect to policymaking, any specific rules promulgated by the Executive Branch need to comply with the key principles of the statute and must not be solely the product of the implementing agencies. While agencies should be allowed to contribute to the development of these rules, final authority must reside elsewhere, in a forward-thinking body of innovative members engaged in continual reassessment of the appropriateness and effectiveness of these policies. Recognizing the critical role of staff in such an organization, this body would benefit immeasurably from a permanent staff with the necessary expertise and independence from affected agencies.

The policymaking process must also become more open. Only on the rarest of occasions when classified information must be discussed should representatives of outside organizations be prohibited from attending. In addition, the President should work to fill the remaining positions on the Security Policy Advisory Board with individuals who would bring the "non-governmental and public interest perspective" that the President intended the Advisory Board to provide. Likewise, the President should promptly appoint the Information Security Policy Advisory Council so that it may begin to advise the President on Executive Order 12958.

Oversight should be the responsibility of a strong and active organization, independent of the agencies that classify, perhaps modeled after agency inspectors general offices. To be truly effective, such an organization should also possess the means to compel agency compliance with established policies. One possibility would be to empower it with some form of limited budgetary authority—such as the review and certification of agencies' expenditures for classification and declassification activities before they are submitted to the Office of Management and Budget (OMB). A greater willingness on the part of both the National Security Council and OMB officials to question the classification of the documents they receive could provide an additional incentive for senior agency officials to address classification matters more seriously. Equally critical is that such a body have adequate resources, whether through a budget line item or the reallocation of resources from the principal classifying agencies.

The Commission believes that classification and declassification policy and oversight should not be viewed solely as security matters. Instead, they should be viewed primarily as information management issues which require personnel with subject matter and records management expertise. In addition, classification and declassification are unique in that, unlike many security issues, they profoundly affect numerous individuals and organizations outside the Government.

Under the statutory approach recommended in Chapter I, the President would retain the authority to establish policymaking and oversight mechanisms to fulfill the basic principles of the legislation. Therefore, the Commission envisions that this recommendation could be achieved by an executive order modifying either Executive Order 12958 (which sets out the responsibilities of the ISOO) or Presidential Decision Directive 29 (which sets out the responsibilities of the SPB), or both.

Recommendation

The Commission recommends that responsibility for classification and declassification policy development and oversight be assigned to a single Executive Branch body, designated by the President and independent of the agencies that classify. This entity should have sufficient resources and be empowered to carry out oversight of agency practices and to develop policy. Based on its oversight findings, this body would then make recommendations for policy and implementation of classification and declassification issues directly to the National Security Council. The Security Policy Board would have an opportunity to comment on these policy recommendations through the NSC process.

Strengthening Implementation and Oversight Within Agencies

Beyond restructuring the incentives for individual classifiers, as suggested above, oversight within agencies can be enhanced through periodic audits and reviews by agencies of their own classified product. However, executive orders have long failed to distinguish clearly between oversight and review of classification management practices and oversight of security practices generally. Those that do occur still focus more on the *safeguarding* of already classified information than on whether the information was properly classified in the first place or whether classification is still warranted at later stages of a document's life cycle.[33] The past decade has seen a steady decline in even these limited inspections.

Agencies are now required by Executive Order 12958 to institute ongoing self-inspection programs, including the periodic review and assessment of their classified product. Under the Order's implementing directive, however, such reviews are only one of several options that agencies "may include" in their program. Many agencies still fail to devote sufficient resources and personnel to reviewing their own practices and classified product. In contrast, the recently developed Information Management Audit and Improvement Program at the CIA serves as a model for how to implement an oversight program. Following audits to evaluate compliance with classification and records management policies, auditors intend to work with staff in a non-punitive manner to improve compliance. Citing the "many benefits" they provide, the ISOO has pointed out that "document reviews highlight an individual agency's performance in classifying and marking documents and suggest areas in need of improvement."[34]

Each agency with the authority to classify would benefit from an established program, subject to minimum Executive Branch standards, for regular evaluations of its classification and declassification decisions, including the review of representative samples of agency classified materials. Such evaluation programs would help foster a nonpunitive approach to improving the quality of classification decisions. Improved agency evaluations, which could be implemented by an agency ombudsman (as suggested in Chapter III), could serve as the basis for outside review of an agency's classification program. In addition, a greater willingness on the part of agency executive secretaries to question the classification assignments of the documents they receive could provide an additional incentive for personnel throughout those agencies to classify properly.

Conclusion

As in the past, the ability of the United States to defend its national security interests in the future will depend, in part, on its ability to maintain the confidentiality of certain information. The ability of the public to obtain information about the activities and operations of its government will depend, in part, on limiting that secrecy to only those activities that truly require it. Paradoxically, today's secrecy system fails to meet either of these goals effectively.

To improve existing practices, senior officials across all the agencies that classify must exert greater leadership and make it clear to subordinates that reducing secrecy, consistent with national security concerns, is a priority. Policies that either implicitly or explicitly encourage classification without much thought to the consequences of that

decision must give way to those that encourage a more balanced consideration of the need for secrecy. Those who classify must be instructed and then evaluated on how they approach their classification responsibilities. Classifiers must be aware that classification means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to information that would be unnecessary if the information were not classified. The tools designed to assist those classifiers, including classification guides, must be readily available and reflect current national security realities. Underlying all these reforms is the need for a more stable and consistent classification regime, which over fifty years of Executive Branch regulation has been unable to provide.

The age-old struggle to find the proper equilibrium between the need for secrecy in certain instances and the need for open government will by no means end with this Commission. Still, the proposals set out above have the potential to reorient the secrecy system to reflect the fact that reducing secrecy and protecting core national secrets are not exclusive of, but instead dependent upon, one another.

---

[1] The President has designated the following 29 officials (including himself) as having the authority to classify originally: Vice President, Chief of Staff to the President, Director of OMB, National Security Advisor, Director of the Office of National Drug Control Policy, Chairman of the President's Foreign Intelligence Advisory Board; Secretaries of State, Treasury, Defense, Army, Navy, Air Force, Energy, Commerce, and Transportation; Attorney General; Chairman of the Nuclear Regulatory Commission, Director of the Arms Control and Disarmament Agency, Director of Central Intelligence, Administrator of the National Aeronautics and Space Administration, Director of the Federal Emergency Management Agency, U.S. Trade Representative, Chairman of the Council of Economic Advisors, Director of the Office of Science and Technology Policy, Administrator of the Agency for International Development, Director of the U.S. Information Agency, President of the Export-Import Bank of the United States, and the President of Overseas Private Investment Corporation; and Information Security Oversight Office, *1995 Report to the President* (Washington, D.C.: Information Security Oversight Office, 1996), 16.

[2] *New York Times Co. v. United States*, 403 U.S. 713, 729 (1971) (concurring opinion).

[3] Peter Hernon, "Information Life Cycle: Its Place in the Management of U.S. Government Information Resources," *Government Information Quarterly* 11, no. 2 (1994): 147, quoting General Services Administration, Information Resources Management Service, *Applying Technology to Record Systems: A Media Guideline* (Washington, D.C.: May 1993), 45.

[4] National Archives and Records Administration, *Draft "Requirements for Electronic Recordkeeping in the Office Environment* (College Park: National Archives and Records Administration, 1996), 4.

[5] Joint Security Commission, *Redefining Security* (Washington, D.C.: 1994), 5.

[6] Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, D.C.: Government Printing Office, 1995), 88.

[7] National Academy of Sciences Panel on DoE Declassification Policy and Practice, Committee on International Security and Arms Control, *Review of the Department of Energy's Response to the Recommendations in the National Research Council Study of DoE Declassification Policy and Practice* (Washington, D.C.: National Academy of Sciences, July 1996), 15-21.

[8] Meridian Corporation, *Classification Policy Study* (Washington, D.C.: Department of Energy, 4 July 1992), 56; National Research Council, *A Review of the Department of Energy Classification Policy and Practice* (Washington, D.C.: National Academy Press, 1995), 90; Department of

Energy, *Openness...Creating a Legacy: Fundamental Classification Policy Review, Draft Report for Public Comment* (Washington, D.C.: Department of Energy, 2 February 1996), 22. In a 1996 follow-up to their 1995 report, the National Research Council explained that an additional problem with FRD is the difficulty of obtaining interagency agreement on which information is to be transclassified and declassified. According to the NRC, "relatively low-ranking staff members from other [non-DoE] agencies may be able to block proposed. . . actions for inappropriate reasons." (National Academy of Sciences Panel on DoE Declassification Policy and Practice, Committee on International Security and Arms Control, *Review of the Department of Energy's Response,* 9).

[9] National Research Council, *A Review of the Department of Energy Classification Policy and Practices*, 48.

[10] Averages for years 1990-1995, as reported by the Information Security Oversight Office.

[11] Among the first was the 1957 Commission on Government Security, which called for the outright abolition of the Confidential level (The Commission on Government Security, *Report of the Commission on Government Security* [Washington, D.C.: Government Printing Office, 1957], 176). Although it did not call for its abolition, the 1970 Seitz Task Force called the Confidential level "probably useless" as applied at the time to research and development (Defense Science Board, Task Force on Secrecy, *Report of the Defense Science Board: Task Force on Secrecy* [Washington, D.C.: Office of the Director of Defense Research and Engineering, 1 July 1970], 10). The initial draft of what would later become Executive Order 12958 also eliminated the Confidential level. However, it was retained out of concerns that (1) the military services, which use a great deal of Confidential information, would be forced to spend enormous sums of money replacing safes so that the information could be protected at the Secret level, and (2) doing so could jeopardize prior or pending prosecutions under the Espionage Act.

[12] The 1957 Commission on Government Security pointed out disagreement over how effectively the need-to-know principle was being implemented (Commission on Government Security, *Report of the Commission on Government Security,* 313). By 1984, ISOO found "widespread indifference" to the principle (Information Security Oversight Office, *Annual Report to the President for FY 1984* [Washington, D.C.: Information Security Oversight Office, 1985], 23). In 1994 the Joint Security Commission stated that the classification system "does not adequately enforce the 'need-to-know' principle" (Joint Security Commission, *Redefining Security,* 8).

[13] Controlled Access Program Oversight Committee (CAPOC), Community Management Staff official, interview by Commission staff, June 1996; Office of the Under Secretary of Defense for Policy Support officials, interview by Commission staff, June 1996.

[14] This Commission requested information from all thirteen Cabinet-level departments and 34 agencies thought most likely to generate sensitive unclassified information. Of the twelve departments and 32 agencies that responded, nine departments and 30 agencies stated that they generate such information.

[15] Office of the Assistant Deputy to the Under Secretary of Defense (Policy) for Policy Support officials, interview by Commission staff, 22 May 1996.

[16] A 1956 report commissioned by the Secretary of Defense recommended that DoD reduce the number of individuals with the authority to classify information as Top Secret (Department of Defense, Committee on Classified Information, *Report to the Secretary of Defense by the Committee on Classified Information* [Washington, D.C.: Department of Defense, 8 November 1956], 6). The 1985 Stilwell Commission report called for "further reductions" in the number of Original Classification Authorities at the Department of Defense (The Commission to Review DoD Security Policies and Practices, *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices* [Washington, D.C.: Department of Defense, 1985], 49).

[17] Information Security Oversight Office, *1995 Report to the President*, 11.

[18] Average for years 1990-1995, as reported by the Information Security Oversight Office.

[19] Information Security Oversight Office official, interview by Commission staff, June 1996.

[20] The General Accounting Office first stated in 1979 that the practice of allowing personnel to classify derivatively through the use of guides "seriously weakens control over the classification process because it allows thousands of individuals who are not designated as classifiers to be involved in the process without being personally accountable" (General Accounting Office, *Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program*, LCD-78-125 [Washington, D.C.: General Accounting Office, 9 March 1979], iv).
[21] Steven Garfinkel, letter to Chairman Lee Hamilton, Subcommittee on Europe and the Middle East, Committee on Foreign Affairs, Washington, D.C., 4 August 1989. The letter responded to inquiries by Chairman Hamilton concerning the operation of the classification system.
[22] Morton Halperin, meeting with Commission staff, 19 October 1995.
[23] The Joint Security Commission argued that a "less complicated system can help correct the current approach that has led to classifying too much at too high a level and for too long" (*Redefining Security*, 10).
[24] Steven Garfinkel, Director, Information Security Oversight Office, stated at a May 5, 1982, congressional hearing that "about 5 percent of the documents [ISOO] review[s] clearly don't merit classification" (House Committee on Government Operations, *Security Classification Policy and Executive Order 12356, Committee on Government Operations,* 97th Cong., 2d sess., 12 August 1982, 44). In 1992 ISOO reported that its review of nearly 11,000 classified documents revealed that only 1.5 percent should not have been classified, and the need for another 1.7 percent was "questionable" (Information Security Oversight Office, *Report to the President for FY 1992* [Washington, D.C.: Information Security Oversight Office, 1993], 9). In 1996 Director Garfinkel stated to Commission staff that the problem of unnecessary classification ranges between 5 and 10 percent "at most" (interview by Commission staff, 15 May 1996).
[25] Inspector General, Department of Defense, *White Paper: Classification and Declassification Within the Department of Defense* (Washington, D.C.: Department of Defense, May 1995), letter of transmittal and page i.
[26] Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary and Subcommittee on Civil Service, Committee on Post Office and Civil Service *Preliminary Joint Staff Study on the Protection of National Secrets,* 48.
[27] Thomas P. Coakley, ed., *C^3I: Issues of Command and Control* (Washington, D.C.: National Defense University Press, 1991), 94.
[28] National Research Council, *A Review of the Department of Energy Classification Policy and Practices*, 89.
[29] National Academy of Sciences, *A Review of the Department of Energy's Response*, 6.
[30] President, Presidential Decision Directive 29, "Security Policy Coordination" (15 September 1994), 2.
[31] When created by President Carter's Executive Order 12065, the ISOO was placed within the General Services Administration and received general policy direction from the National Security Council. In FY 1995, the ISOO was moved to the Office of Management and Budget (OMB) as a result of an attempt within Congress to place the office within the NSC—a move that sparked concerns that the ISOO's oversight activities would conflict with the NSC's policymaking role. However, some OMB officials strongly opposed having the ISOO based within the OMB, and Congress in turn transferred the ISOO to NARA beginning in FY 1996. During FY 1996, the ISOO operated on funds earmarked for NARA, which did not receive any additional appropriation to accommodate the ISOO's activities.
[32] Steven Garfinkel, telephone conversation with Commission staff, August 1996.
[33] The three most recent executive orders on classification (Executive Orders 12065, 12356, and 12958) highlight this particularly well. All three orders directed agencies to establish security education and/or training programs to ensure their implementation, but none specified that classification management (to be distinguished from security generally) be included in this training.
[34] Information Security Oversight Office, *Annual Report for FY 1992* (Washington, D.C.: Information Security Oversight Office, 1993), 4.