Formal Statement

J. William Leonard

Director, Information Security Oversight Office

before the House Permanent Select Committee on Intelligence

Subcommittee on Intelligence Community Management

U.S. House of Representatives

July 12, 2007

Chairwoman Eshoo, Mr. Issa, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to classification of national security information within the Intelligence Community as well as for inviting me to testify today.

Background

By section 5.2 of Executive Order 12958, as amended, "Classified National Security Information" (the Order), the President established the organization I direct, the Information Security Oversight Office, often called "ISOO." We are within the National Archives and Records Administration and by law and Executive order (44 U.S.C. 2102 and sec. 5.2(b) of E.O. 12958) are directed by the Archivist of the United States, who appoints the Director of ISOO, subject to the approval of the President. We also receive policy guidance from the Assistant to the President for National Security Affairs. Under the Order and applicable Presidential guidance, ISOO has substantial responsibilities with respect to the classification, safeguarding, and declassification of information by agencies within the executive branch. Included is the responsibility to develop and promulgate directives implementing the Order. We have done this through ISOO Directive No. 1 (32 CFR Part 2001) (the Directive).

The classification system and its ability to restrict the dissemination of information the unauthorized disclosure of which could result in harm to our nation and its citizens represents a fundamental tool at the Government's disposal to provide for the "common defense." The ability to surprise and deceive the enemy can spell the difference between success and failure on the battlefield. Similarly, it is nearly impossible for our intelligence services to recruit human sources who often risk their lives aiding our country or to obtain assistance from other countries' intelligence services, unless such sources can be assured complete and total confidentiality. Likewise, certain intelligence methods can work only if the adversary is unaware of their existence. Finally, the

successful discourse between nations often depends upon confidentiality and plausible deniability as the only way to balance competing and divergent national interests.

It is the Order that sets forth the basic framework and legal authority by which executive branch agencies may classify national security information. Pursuant to his constitutional authority, and through the Order, the President has authorized a limited number of officials to apply classification to certain national security related information. In delegating classification authority the President has established clear parameters for its use and certain burdens that must be satisfied.

Specifically, every act of classifying information must be traceable back to its origin as an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, the original classification authority must be able to identify or describe the damage to national security that could reasonably be expected if the information was subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the control of the U. S. Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.[1]

The President has also spelled out in the Order some very clear prohibitions and limitations with respect to the use of classification. Specifically, for example, in no case can information be classified in order to conceal violations of law, inefficiency, or administrative error, to restrain competition, to prevent embarrassment to a person, organization, or agency, or to prevent or delay the release of information that does not require protection in the interest of national security.

It is the responsibility of officials delegated original classification authority to establish at the time of their original decision the level of classification (Top Secret, Secret, and Confidential), as well as the duration of classification, which normally will not exceed ten years but in all cases cannot exceed 25 years unless an agency has received specific authorization to extend the period of classification.

Changes to the Order Over the Past Decade

The current framework has basically been in effect since 1995. One of the most innovative features of the current framework is the concept of automatic declassification. Under prior executive orders governing classification and declassification, information once classified remained so indefinitely and very often did not become available to

[1] Pursuant to § 1.4 of the Order, information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

general public, researchers, or historians without persistent and continuous effort on the part of these individuals. While all agencies had the responsibility to systematically review historical classified records for declassification, and some agencies such as the State Department did so on a regular basis, there was no specified consequence for agencies that did not conduct such reviews. Understandably, in times of budget constraints, reviews for declassification suffered, resulting in a significant backlog or "mountain" of classified historical records, many of which were much older than 25 years of age.

Under automatic declassification, information in records appraised as having permanent historical value is automatically declassified 25 years after classification, unless an agency head has determined that it falls within one of several limited exceptions that permit continued classification, a continuation that either the President or the Interagency Security Classification Appeals Panel (ISCAP) has approved. In effect, automatic declassification reverses the resource burden. Unlike previous systems, in which agencies had to expend resources to declassify older information, under the current system, agencies must expend resources to demonstrate why older historical information needs to remain classified.

In March 2003, the President signed Executive Order 13292 further amending Executive Order 12958. The principal purpose of the amendment was to provide agencies an additional three and a half years to address the remaining backlog of unreviewed 25-year-old classified records of permanent historical value prior to the onset of automatic declassification. This and other changes were recommended by a broad consensus of interagency professionals in classification and declassification. They reflect seven years of experience in implementing E.O. 12958 as well as new priorities resulting from the events of 9/11.

What is most notable about the 2003 amendment is what did not change. The revision left the existing classification/declassification regime largely intact. It had an exceedingly limited impact on the way in which government officials classified or declassified information. For all practical purposes, it institutionalized automatic declassification as an essential element of the classification process.

For classifiers, the most notable change was a simplification of the process and a resulting change in marking requirements. For those involved in the declassification process, in addition to providing more time to complete the review of 25-year old records, the revision gave greater clarity to what records are subject to automatic declassification and under what conditions.

A synopsis of the most significant changes included in the amendment is set forth below:

- Deadline for Automatic Declassification Extended. The 2003 amendment committed agencies to finish reviewing the backlog of classified records more than 25 years old, by the end of 2006. (Sec. 3.3(a))

- Clarification of Documents Subject to Automatic Declassification. Before the most recent amendment, the language of the Order was unclear as to what 25-year-old documents that had not been explicitly exempted from release were subject to declassification and under what circumstances. Moreover, even in blocks of retired records spanning a period of years, the language suggested that older documents would become automatically declassified before the larger body of records was subject to review.

  A number of changes were made that clarified the question of what documents are automatically declassified at 25 years:
  - records in a file block shall not be automatically declassified until the most recent record is 25 years old (Sec. 3.3(e)(1));
  - an additional five years is allowed for difficult to review records such as audio and video tapes (Sec. 3.3(e)(2));
  - an additional three years is allowed for the release of records transferred or referred from another agency (Sec. 3.3(e)(3));
  - an additional three years is allowed for newly discovered records (Sec.3.3(e)(4)).

- Protecting Foreign Government Information. The 2003 amendment to the Order contained the presumption that the unauthorized disclosure of foreign government information exchanged in confidence will cause damage to the national security (Sec. 1.1(c)). The practical consequence of this addition was limited since the original Order contained such broad discretion in this area that an original classifier had the authority to classify such information all along. More importantly, the amendment made it explicit that for foreign government information to be exempt from automatic declassification, the same standard as other information concerning foreign and diplomatic relations of the United States and a foreign government is to be applied. Specifically, serious and demonstrable "impairment" or "undermining" of these relations or activities must be shown in order for the information to be exempted. (Sec 3.3(b)(6))

- Categories of Classifiable Information Clarified. Additional categories of information, specifically defense against transnational terrorism, infrastructures, and protection services, were explicitly spelled out as included in those that were eligible for classification. "Weapons of mass destruction" was added as a separate category. Arguably, all such information was already covered by the existing Order but the amendment made these points clearer. (Sec. 1.4 (e) (g) & (h))

- Simplifying the Scheme. E.O. 12958 had been considered unduly complicated to administer because of separate criteria for original classification for up to ten years; for original classification from 10 to 25 years; and for extending classification beyond 25 years. To correct this, the separate set of criteria for withholding information between 10 and 25 years from date of origin was eliminated. While the revised language maintains ten years as the norm for most original classification actions,

there is now one set of criteria for classification up to 25 years (Sec. 1.4) and another for continuing classification beyond 25 years (Sec. 3.3(b)).

- Reclassification of Properly Released Material. As originally issued, the Order prohibited the reclassification of information after it had been released to the public under proper authority and prohibited it entirely for documents more than 25 years old. The 2003 amendment restored the ability under the predecessor executive order to reclassify such information and dropped the prohibition on 25-year-old information, but only under "the personal authority of the agency head or deputy agency head" and only if the material may be "reasonably recovered." (Sec. 1.7(c) & (d))

- Continuing Ability to Exempt File Series. When the order was originally issued in 1995, it required that all record file series that were to be exempted from automatic declassification at 25 years be identified to the President before the Order went into effect. This was changed so that an agency may now notify the President at any time of file series of records that qualify under the specific standards for exemption. (Sec. 3.3(c))

- Authority of Director of National Intelligence (DNI) Recognized. While intelligence sources and methods information remain subject to the jurisdiction of Interagency Security Classification Appeals Panel (ISCAP), the amendment recognized the special authority and responsibility of the now DNI to protect such information. As such, this revision authorized the DNI to object to final ISCAP declassification conclusions about such information. Furthermore, a decision by the DNI to bar release can still be appealed to the President by any member agency of ISCAP. (Sec. 5.3(f))

- Sharing Classified Information in an Emergency. One of the issues that arose in the wake of 9/11 was awareness of the limitations imposed by the lack of authority under the Order to pass classified information to individuals not otherwise eligible (e.g. local and state authorities without the necessary clearances) in an emergency. As a result, a section was added specifically authorizing an agency head or designated person to share classified information with individuals not otherwise eligible to receive it and specifying procedures to be followed. (Sec 4.2(b))

Agency Compliance With the Order

In fiscal year (FY) 2006, pursuant to sections 5.2(b)(2) and (4) of E.O. 12958, as amended, my office conducted a total of 15 onsite reviews of Executive branch agencies. Most of these reviews evaluated the agencies implementation of the classified national security information program to include such core elements as organization and management, classification and declassification, security education and training, self-inspections, safeguarding practices, classification markings, and security violations procedures.

Of the general program reviews we conducted last fiscal year, we found that few of the agencies visited had adequately implemented the core elements of the classified national security information program. Shortcomings were observed at multiple agencies in their implementing regulations, self-inspection programs, document markings, and refresher security education and training. It is disappointing to note that these same shortcomings were noted in FY 2004 and 2005. I should note that as a general rule, intelligence community agencies tend to have the most sound information security programs within the Executive branch.

At several agencies, the ISOO onsite reviews identified inadequate support from senior management for the information security program. Sections 5.4 (a) and (b) require agency heads and senior management of agencies that originate or handle classified information to demonstrate commitment and consign necessary resources to the effective implementation of the Order.

An area of significant concern was the failure of agencies to update their regulations that implement E.O. 12958, as amended, even though the Order was amended in 2003. Implementing regulations are essential to the program because they are the foundation for agency personnel in terms of obtaining guidance and procedures pertinent to their individual responsibilities under the Order and the Directive.

As found in FYs 2004 and 2005, many agencies have not established comprehensive self-inspection programs. The primary reason for the shortcomings of these agencies' self-inspection programs were inadequate staffing levels necessary to meet their internal oversight responsibilities and insufficient senior agency official emphasis. Self-inspections are an important element of the information security program because they enable the agency to evaluate, as a whole, its implementation of the Order's program and make adjustments and corrective action, as appropriate.

Refresher security education and training, although an annual requirement of the Order, was not being provided at a few of the agencies reviewed. This training is fundamental to the continuous reinforcement of the policies, principles, and procedures that individuals authorized access to classified information are expected to understand and implement.

In FY 2006, we concentrated much of our compliance reviews on the appropriateness of classification decisions. We focused on evaluating if agencies were correctly applying the Order's standards for originally and derivatively classifying information. Unfortunately, the reviews revealed source information often could not be tracked when "multiple sources" was entered on the "derived from" line of the document classification block. Almost all agencies reviewed were not keeping a list of the source documents with the file or record copy as required by the Directive. In addition, we found a high percentage of documents with an unknown basis for classification, as these documents failed to indicate the authority or basis for classification, thereby calling into question the propriety of their classification. To make clear to the holder the basis for classification and to facilitate information sharing and automatic declassification, it is imperative that

multiple sources are listed and the basis for classification is identified when designating national security information as being classified.

Another area of concern was the failure of agencies to review and update their security classification guidance at least every five years or sooner as circumstances require. In large part due to lack of timely revision to classification guides, agencies were still using obsolete X1-X8 declassification markings, which were eliminated by the 2003 amendment to the Order. As a consequence of this erroneous action, the accuracy and appropriateness of subsequent derivative classification determinations based upon such improperly marked documents is placed in jeopardy.

As part of our onsite reviews, we review a sample of documents to ascertain compliance with requirements set forth in the Order and Directive. A review by ISOO of over 2000 documents in FY 2006 revealed the following:

- nearly 39 percent had errors with regard to declassification instructions;
- portion markings were inconsistently applied in over 30 percent of the documents; and
- for over 11 percent of the documents, the basis for classification could not be identified.

An essential requirement of the Order is that only an original classification authority (OCA) is authorized to classify information in the first instance. Thus original classifications can only be made by an OCA, and every derivative classification decision must be able to be traced to a source document or classification guide. The consequence of having so many documents for which the basis of their classification could not be determined is that any future classification decisions based upon these same documents will be equally problematic and their true classification status uncertain.

When an agency fails to effectively implement one or more elements of the classified national security program, it weakens its entire program because each of the elements has an essential purpose that is interdependent upon the others. Implementing regulations set the foundation for the program and establish the agency framework to implement the Order. Deficiencies in regulations lead to gaps in the agency's implementation of the program. Classification guides are a critical tool that prescribes the classification of specific information. They identify the elements of information regarding a specific subject that must be classified and establish the level and duration of classification for each element. Outdated classification guides may reproduce numerous invalid derivative classification decisions, thereby undermining the classification system provided by the Order. It is imperative that classification guides are updated to reflect the changes of the Order and otherwise be kept current.

Security education and training briefings inform/remind agency personnel of their duties and responsibilities and on the proper procedures for creating, handling, and destroying classified information. Inadequately trained personnel are more prone to mistakes while working with classified information. Self-inspections enable an agency to evaluate the implementation of its program on a regular basis, identify areas of concern, and take

corrective action, as applicable. The absence of a self-inspection program can leave problems unidentified and uncorrected and eventually place national security information at risk. For an effective program, the various program elements must work together.

Impacts of Overclassification

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified, or is not classified in the first place although clearly warranted, our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations can be subject to potential harm. Conversely, too much classification, the failure to declassify information as soon as it no longer satisfies the standards for continued classification, or inappropriate reclassification, unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government. In the final analysis, inappropriate classification activity of any nature undermines the integrity of the entire process and diminishes the effectiveness of this critical national security tool. Consequently, inappropriate classification or declassification puts our most sensitive secrets at needless increased risk.

Classification, of course, can be a double-edged sword. Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk of a lack of awareness on the part of our own forces, contributing to the potential for friendly fire incidents or other failures. Similarly, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government. Simply put, secrecy comes at a price. I have continuously encouraged agencies to become more successful in factoring this reality into the overall risk equation when making classification decisions.

Classification is an important fundamental principle when it comes to national security, but it need not and should not be an automatic first principle. The decision to originally classify information in the first instance or not is ultimately the prerogative of agency original classification authorities. The exercise of agency prerogative to classify certain information, of course, has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with another agency, with State or local officials, or with the public, if they need to know the information.

The challenge of overclassification is not new. Over 50 years ago, Congress established the Commission on Government Security (known as the “Wright Commission”). Among its conclusions, which were put forth in 1955, at the height of the Cold War, was the observation that overclassification of information in and of itself represented a danger to national security. This observation was echoed in just about every serious review of the classification systems since to include: the Commission to Review DoD Security Policies and Practices (known as the “Stillwell Commission”) created in 1985 in the wake of the Walker espionage case; the Joint Security Commission established during the aftermath of the Ames espionage affair; and the Commission on Protecting and Reducing

Government Secrecy (often referred to as the "Moynihan Commission"), which was similarly established by Congress and which issued its report in 1997.

More recently, the National Commission on Terrorist Attacks on the United States (the "9-11 Commission"), and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "WMD Commission") likewise identified overclassification of information as a serious challenge.

As I stated earlier, the ability and authority to classify national security information is a critical tool at the disposal of the Government and its leaders to protect our nation and its citizens. In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool. To be effective, the classification process is a tool that must be wielded with precision. In an audit of agency classification activity conducted by my office over a year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it clearly right only 64 percent of the time in making determinations as to the appropriateness of classification. This is emblematic of the daily challenges confronting agencies when ensuring that the 3 million plus cleared individuals with at least theoretical ability to derivatively classify information get it right each and every time.

Effectiveness of Current Declassification Efforts

Setting deadlines for agency action in implementing the automatic declassification provisions of the Order is essential in ensuring the continued integrity and effectiveness of the classification system, which cannot be depended upon to protect today's sensitive national security information unless there is an ongoing process to purge it of yesterday's secrets that no longer require protection. The automatic declassification process increases the potential release of formerly classified information to policy-makers and lawmakers as well as the general public and researchers, enhancing their knowledge of the United States' democratic institutions and history, while at the same time ensuring that information which can still cause damage to national security continues to be protected. An agency's failure to fully implement automatic declassification provisions undermines its ability to achieve these complementary objectives.

After several deadline extensions, automatic declassification finally became effective on December 31, 2006, with a few notable authorized delays. While a detailed analysis of the final results is still underway, it appears that all Executive branch agencies have succeeded in meeting their obligations under the automatic declassification provisions of the Order. As significant as the initial development of the concept of automatic declassification was, its actual implementation after so many false starts and delays is even more of an accomplishment. It reflects well on the diligence and efforts of both the public servants who accomplished this milestone through their hard work and perseverance, as well as the agencies that committed the requisite resources. I should note to you today the significant leadership and support within the interagency declassification community displayed by the Central Intelligence Agency since 1995.

Significant challenges remain. For example, the Order allows a delay in automatic declassification for up to three additional years (December 31, 2009, for classified records currently 25-years-old or older) that contain information of more than one agency or information the disclosure of which would affect the interests or activities of other agencies. Similarly, automatic declassification for classified information contained in microforms, motion pictures, audio tapes, video tapes, or comparable media that make a review for possible declassification exemptions more difficult or costly may be delayed from automatic declassification for up to five additional years. Improved processes, education about other agency equities and enhanced agency collaboration are necessary to ensure quality reviews with minimal referrals and adequate documentation regarding actual decisions made are essential.

It should be noted that from the perspective of the public, researchers and historians, there is no "vault-full" of previously classified records that became automatically publicly available on January 1, 2007. However, in many regards, the public has already seen the major benefits of automatic declassification. Automatic declassification has served as the impetus during the recent past (since 1995) for many agencies to devote necessary resources for the establishment of substantial ongoing declassification review programs.

During FY 2006, the Executive branch declassified 37,647,993 pages of permanently valuable historical records, which is a 27 percent increase over what was reported for FY 2005. This large increase was primarily due to the final push to comply with the December 31, 2006 automatic declassification deadline. Since 1995, agencies have reported the declassification of more than 1.33 billion pages of previously classified historical records. Only 257 million pages were declassified under the two previous executive orders governing classified information, a period encompassing almost twice as many years.

Furthermore, the infrastructures established by agencies to accomplish declassification reviews since 1995 will continue indefinitely, thus contributing to the universe of declassified information as a new batch of historical records reaches 25-years of age each and every year. However, we are concerned that some agencies may have regarded the automatic declassification deadline of December 31, 2006 as a one-time push rather than an ongoing requirement.

Finally, declassification does not always equate to public access. Documents that have been declassified must still be reviewed to ascertain whether they contain other information that may not be releasable to the public, e.g. personal information. Also, declassified records must be accessioned and processed by archivists before they can be "put on the public shelves." These activities ensure that the National Archives and Records Administration (NARA) has both physical and intellectual control of the records. While some 460 million declassified pages of federal records have been made publicly accessible since 1996, NARA holds another 400 million pages of declassified federal records that require additional processing before they can be made available. To add to

the burden, hundreds of millions of pages, both classified and recently declassified, remain within the custody of their originating agencies and will also require processing upon accession into NARA before they are made available to the public.

Effect of Selective Classification and Declassification

As I indicated earlier, the decision to originally classify information in the first instance or not is ultimately the prerogative of agency original classification authorities.

Similarly, the Order clearly states that information shall be declassified as soon as it no longer meets the standards for classification under this order, irrespective of the initial duration decision of the original classification authority. The Order goes on to state (section 3.1 (b)) that it is presumed that information that continues to meet the classification requirements under the Order requires continued protection. However, the Order does recognize that in some exceptional cases the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, the Order assigns the responsibility to make such a decision to the agency head or the senior agency official designated by the agency head under the Order. That official is responsible to determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.

Again, I thank you for inviting me here today, Madame Chairwoman, and I would be happy to answer any questions that you or the subcommittee might have at this time.