Formal Statement

J. William Leonard

Director, Information Security Oversight Office

before the Committee on Homeland Security

Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

U.S. House of Representatives

March 22, 2007

Chairwoman Harman, Mr. Reichert, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to the very real challenge of overclassification of information within the Federal Government as well as for inviting me to testify today.

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 would 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.

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 today's most sensitive secrets at needless increased risk.

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 (otherwise known 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

It is Executive Order 12958, as amended, 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

[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.

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.

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. Few, if any, both within and outside Government, would deny that too much of the information produced by our agencies is classified. In an audit of agency classification activity conducted by my office approximately one 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.

In response to the findings of this audit, last year I wrote to all agency heads and made a number of recommendations for their consideration. Collectively, these recommendations help preserve the integrity of the classification system while at the same time reduce inefficiencies and cost. They included:

- Emphasizing to all authorized holders of classified information the affirmative responsibility they have under the Order to challenge the classification status of information that they believe is improperly classified (§1.8(a) of the Order).

- Requiring the review of agency procedures to ensure that they facilitate classification challenges (§1.8(b) of the Order). In this regard, agencies were encouraged to consider the appointment of impartial officials whose sole purpose is to seek out inappropriate instances of classification and to encourage others to adhere to their individual responsibility to challenge classification, as appropriate.

- Ensuring that quality classification guides of adequate specificity and clarity are prepared and updated to further accurate and consistent derivative classification decisions (§2.2 of the Order).

- Ensuring the routine sampling of recently classified information to determine the propriety of classification and the application of proper and full markings (§5.4(d)(4) of the Order). Consideration should be given to reporting the results of these reviews to agency personnel as well as to the officials designated above who would be responsible to track trends and assess the overall effectiveness of the agency's efforts and make adjustments, as appropriate.

- Ensuring that information is declassified as soon as it no longer meets the standards for classification (§3.1(a) of the Order).

- Ensuring that prior to exercising the national security exemption as set forth in 5 U.S.C. 552b(1) when responding to FOIA requests, that agency personnel verify that the information involved clearly meets the standards for continued classification irrespective of the markings, to include declassification instructions, contained on the document.

Recognizing that a focus of this hearing includes policies and procedures for handling sensitive unclassified information, it is important to articulate recent initiatives by the President to ensure the robust and effective sharing of terrorism information vital to protecting Americans and the Homeland from terrorist attacks. To that end, the President has promulgated a set of guidelines and requirements that represent a significant step in the establishment of the Information Sharing Environment (ISE) called for by section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

Specifically, to promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, the President has mandated the standardization of procedures for designating, marking, and handling SBU information across the Federal Government. A clear mandate for achieving this goal has been laid out for the entire Executive branch and significant progress is underway to develop for the President's consideration standardized procedures for handling controlled unclassified information. Once implemented, our nation's defenders will be able to share controlled unclassified information more rapidly and confidently. The existence of such an option should significantly reduce the incentive to overclassify information. This happens now, in part, due to the absence of a dependable regime for the proper protection of sensitive information which should not be classified.

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.