FORMAL STATEMENT

J. William Leonard
Director, Information Security Oversight Office
National Archives and Records Administration

before the
Committee on Government Reform
Subcommittee on National Security, Emerging Threats,
and International Relations
U.S. House of Representatives
March 2, 2005

Chairman Shays, Mr. Kucinich, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to information access restrictions as well as for inviting me to testify today.

Our Nation and its Government are, of course, profoundly different in a post-9/11 world. Our citizens' sense of vulnerability has increased, as have their expectations of their Government to keep them safe. In each situation, information is crucial. On the one hand, Americans are concerned that information may be exploited by our country's adversaries to harm us. On the other hand, impediments to information sharing among Federal agencies and with State, local and private entities need to be continuously addressed in the interests of homeland security. Even more so, the free flow of information is essential if citizens are to be informed and if they are to hold their

Government and its leaders accountable through informed participation in our electoral processes. In many regards, our Government is confronted with the twin imperatives of information sharing and information protection – two responsibilities that contain inherent tension but are not incompatible.

By section 5.2 of Executive Order 12958, as amended, "Classified National Security Information," 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 supervised by the Archivist of the United States, who appoints the Director, ISOO with the approval of the President. Under Executive Orders 12958 and 12829 (which established the National Industrial Security Program) and applicable Presidential guidance, the ISOO has substantial responsibilities with respect to classification of information by agencies within the executive branch.

It is Executive Order 12958, as amended, that sets forth the basic framework and legal authority by which executive branch agencies classify national security information. Pursuant to his constitutional authority, in this Order the President authorizes a limited number of officials to apply classification to certain national security related information. This authority is an essential and proven tool for defending our nation. 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 constructive ambiguity and plausible deniability as the only way to balance competing and divergent national interests.

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. In certain circumstances, even with respect to national security information, classification can run counter to our national interest. The decision to classify information 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, who genuinely need to know the 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 able to trace its origin to 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 would arise if the information were 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]

As I testified the last time I appeared before this subcommittee, it is my view that the Government classifies too much information; primarily, I believe, because classification often becomes an automatic decision rather than an informed, deliberate decision. My conclusion that there is excessive classification is supported, in part, by agency input 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.

my office that indicates that overall classification activity has risen steadily over the past several years. For example, based upon information furnished our office, the total number of classification decisions increased from 9 million in FY 2001 to 11 million in FY 2002, 14 million in FY 2003 and 16 million in FY 2004. For the sake of precision, I would note that, during the period from FY 2002 through FY 2004, the U.S. Government built a new structure for homeland security and engaged in wars in Afghanistan, Iraq and against al-Qaeda, so it cannot be said conclusively from these data that the increase during this period in the number of classification decisions was due solely or even substantially to the phenomenon of "over classification" as opposed to simply reflecting an increase in legitimate classification decisions as a result of the increase in the tempo of national security operations.

My official oversight responsibilities rest solely with classified national security information and do not extend to the various information access restriction designations used by agencies to control some unclassified information. Nonetheless, as a minimum, I believe the following are proven effective attributes of the classification system:

- Specificity with respect to what information is covered and what is not covered.
- Strict limitations as to who can designate information as falling under the system of controls.
- Built-in discretion that allows controls not to be applied even if the information is eligible.
- Built-in criteria that must be satisfied in order to place controls on dissemination.

- Clear designation of information requiring control to include information orally disseminated.

- Uniform standards with respect to how to handle and protect controlled information.

- A fixed duration of time for the application of controls.

- An appeal procedure whereby both authorized holders and outsiders can appeal the legitimate application of dissemination controls.

- An effective education and training program to maintain awareness.

- Built-in accountability, both for the improper application of controls and the failure to apply or follow legitimate controls.

Finally, we must avoid allowing the "need-to-know" principle to automatically override the “need-to-share” imperative.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the subcommittee might have.