Hearing on
Overclassification and Pseudo-classification: The Impact on Information Sharing

Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
Committee on Homeland Security
United States House of Representatives

Statement of Meredith Fuchs, General Counsel, National Security Archive
March 22, 2007

Chairwoman Harman, Ranking Member Reichert and Members of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, I am honored to appear before you today to talk about the growing problem of government secrecy and the danger it poses to our security.

I am testifying on behalf of the National Security Archive (the "Archive"), a non-profit research institute and leading user of the Freedom of Information Act (FOIA). We publish a wide range of document sets, books, articles, and electronic briefing books, all of which are based on records obtained under the FOIA. In 1999, we won the prestigious George Polk journalism award for "piercing self-serving veils of government secrecy" and, in 2005, an Emmy award for outstanding news research.

In my five years at the Archive, I have overseen five audits of federal agency FOIA processing. Most relevant to this hearing is the report we issued in March 2006 entitled: "Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information."

After the September 11, 2001, attacks on the United States, there were many signs that official secrecy would increase. The attacks themselves led to a wave of legitimate concern about the risks posed by poorly safeguarded government information. Additionally, in March 2002 White House Chief of Staff Andrew H. Card issued a directive to federal agencies requesting a review of all records and policies concerning the protection of "sensitive but unclassified" information. This memorandum spurred agencies to increase controls on information. Further, during times of war or national crisis, the government's tendency to keep secrets always becomes more pronounced and pervasive. Thus, the U.S. entry into hostilities in Afghanistan and Iraq as part of the Global War on Terrorism necessarily led to an increase in the creation of secrets.

The available statistics show that since the September 11 attacks on the United States, there has been a dramatic upsurge in government secrecy. Classification has multiplied, reaching 14.2 million classification decisions in 2005, nearly double the number in 2001. Officials throughout the military and intelligence sectors have admitted that much of this classification activity is unnecessary. Former Secretary of Defense Donald Rumsfeld acknowledged the problem in a 2005 *Wall Street Journal* op-ed: "I have long believed that too much material is classified across the federal government as a general rule. . . ."[1] The extent of over-classification is significant. Under repeated questioning from members of Congress at a hearing concerning over-classification, Deputy Secretary of Defense for Counterintelligence and Security Carol A. Haave eventually conceded that approximately 50 percent of classification

[1] Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12.

decisions are over-classifications.[2] These opinions echoed that of then-Chair of the House Permanent Select Committee on Intelligence Porter Goss, who told the 9/11 Commission, "we overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them."[3]

Alongside traditional classification are a plethora of new non-statutory labels that are being applied to protect information that is deemed sensitive but unclassified. Some estimates count over 100 different so-called "safeguarding" labels for records. There is no way to determine how many records are labeled with safeguarding controls, however, because agencies do not track their use of these labels.

At the same time that the indicators all started to point to increasing secrecy, the numerous investigations into the September 11 attacks on the United States each concluded that excessive secrecy interfered with the detection and prevention of the attacks.[4] Other reports, including one by the Government Accountability Office and one by the successor body to the

[2] *Subcommittee on National Security, Emerging Threats and International Relations of the House Committee on Gov't Reform Hearing*, 108th Cong. (2004) (testimony of Carol A. Haave), http://www.fas.org/sgp/congress/2004/082404transcript.pdf; *See id.*, (Testimony of J. William Leonard, Director of ISOO) ("It is my view that the government classifies too much information.").

[3] *9/11 Commission Hearing*, (Testimony of then Chair of the House Permanent Select Committee on Intelligence Porter Goss) (2003), http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.htm#panel_two.

[4] As the staff director of the Congressional Joint Inquiry on 9/11 found, "[t]he record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and informed American public. One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid." Similarly, the entire 9/11 Commission report includes only one finding that the attacks might have been prevented: "*publicity* about Moussaoui's arrest and a possible hijacking threat might have derailed the plot." Final Report of the National Commission on Terrorist Attacks Upon the United States, at 276 (emphasis added).

9/11 Commission, have decried the delay in establishing a workable information sharing environment.[5]

Against this background, the National Security Archive conducted an extensive audit of the actual policies used by agencies to "safeguard" information.[6] We filed targeted FOIA requests that identified information protection policies of 37 major agencies and components. We obtained and reviewed 28 distinct policies for protection of sensitive unclassified information, many of which allow any employee in the agency to designate sensitive unclassified information for protection, but few that provide any procedure for the labels to be removed. Only a small number of policies included restrictions that prohibit the use of the labels for improper purposes, including to conceal embarrassing or illegal agency actions, or inefficiency. Further, and perhaps most troubling from a security perspective, was the remarkable lack of consistency among agencies as to how to use these labels. Most of the policies were vague, open-ended, or broadly applicable, thus raising concerns about information sharing, the impact of such designations on access to information, free speech, and citizen participation in governance. Given the wide variation of practices and procedures as well as some of their features, it is probable that these policies interfere with interagency information sharing, increase the cost of information security, and limit public access to vital information.

[5] In January 2005, the Government Accountability Office (GAO) added "Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security" to its High Risk List, stating that they were "designating information sharing for homeland security as a government-wide high-risk area because this area, while receiving increased attention, still faces significant challenges" (GAO-05-207). On December 5, 2005, the 9/11 Public Discourse Project, the successor body of the 9/11 Commission, issued its Final Report on 9/11 Commission Recommendations. Important areas on information sharing, including "incentives for information sharing" and "government-wide information sharing," received a D in the scheme of letter grade assessments.

[6] The complete audit report is available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/press.htm.

Further, we concluded that there are almost no incentives to control the use or misuse of these safeguarding labels. Unlike classified records or ordinary agency records subject to FOIA, there is no monitoring of or reporting on the use or impact of protective sensitive unclassified information markings. In comparison, it is useful to look to the formal classification system, which is governed by Executive Order 12958, as amended, and is managed and monitored by the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA). ISOO publishes an annual report to the President in which it quantifies the number of classification and declassification decisions, the number of individuals with authority to classify material, and the type of information that is being classified. Such reports enable the Executive Branch and Congress to monitor the costs and benefits of the classification system and to identify trends that may suggest the need to reform the system.

The absence of reporting mechanisms for sensitive but unclassified control markings makes any assessment of the extent to which a policy is being used difficult, if not impossible. Because safeguarding sensitive unclassified information impacts safety, security, budget and information disclosure—all important national concerns—some form of overarching monitoring of *all* information control would be valuable.

Nor is there a procedure for the public to challenge protective markings. For classified information, the security classification system provides precise limits on the extent and duration of classification as well as a system for declassification, including public requests for declassification. For non-security sensitive information, the FOIA provides a relatively clear and user-friendly process for the public to seek access to information held by the government.

Sensitive unclassified information, however, falls into a black hole. Based on anecdotal information, we believe that information previously available under FOIA or on unrestricted Web sites may no longer be available to the public. Yet, there is virtually no opportunity for the public or other government personnel to challenge a decision to mark a document for protection as SBU, FOUO, or SSI. Accordingly, in order to protect the important role that public access has played in government accountability, it is important that a system for challenging the use of sensitive unclassified information markings be established at each agency or, alternatively, that FOIA procedures be adjusted to counteract the chilling effect these markings may have on disclosure under FOIA.

Congress began to respond to these problems from the outset. Both the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the development of policies for sharing classified and sensitive but unclassified information. IRTPA requires the rapid implementation of an information sharing environment (ISE) to facilitate the government-wide sharing of information about terrorist threats. As the subcommittee is aware, the office of the Program Manager of the ISE was established pursuant to IRPTA to assist, in consultation the Information Sharing Council (ISC), in the development of the ISE. A report and implementation plan for the ISE was required within one year of enactment of IRTPA. President Bush issued a Memorandum on December 16, 2005, directing federal departments and agencies to standardize procedures for handling SBU information.

The President's December 2005 Memorandum setting up the office of the Program Manager contained specific direction related to the standardization of Sensitive But Unclassified

(SBU) information. Specifically, Guideline 3 required each department and agency to inventory existing SBU procedures and their underlying authorities across the Federal government, and to assess the effectiveness of these procedures and provide this inventory and assessment to the Director of National Intelligence (DNI) for transmission to the Secretary of Homeland Security and the Attorney General. The working group completed an initial inventory of SBU designations in March 2006. The original schedule would have resulted in recommendations for submission to the President regarding the standardization of SBU procedures by June 2006. More than 5 years after the September 11 attacks, however, there still is no government-wide plan to standardize information controls and ensure government accountability.

Part of the problem may be that these legislative mandates are being imposed on an executive branch that does not appreciate Congressional interference and does not seem concerned about government accountability. I am reluctant to express such strong sentiments, but the lack of willingness by the Executive Branch to respond to Congress's mandates is strongly evidenced by the refusal of the Office of the Director of National Intelligence to participate in a March 2006 report by the Government Accountability Office about this very matter. In its report, GAO noted that the ODNI "declined to comment on [GAO's] draft report, stating that review of intelligence activities is beyond GAO's purview."

Further, the responsibility for overseeing the development of a comprehensive plan has been shifted from office to office; it was first lodged at the Office of Management and Budget, then at the Department of Homeland Security and now in the Office of the Director of National Intelligence. Thus, despite the urgent need to better coordinate information sharing, it has taken some time for the program to find a home. Whether the ODNI is the proper home remains to be seen, especially in light of that office's unwillingness to be subjected to congressional scrutiny. Another delay was caused by the quick departure of the first Program Manager for the Information Sharing Environment (ISE) in January 2006. He was replaced by Ambassador Thomas McNamara.

I had the opportunity, along with several other open government advocates, to meet with Ambassador McNamara on November 20, 2006. Ambassador McNamara described for our group the challenges that the office of the Program Manager is facing in rationalizing the system for safeguarding records. They must obtain the cooperation of many communities of interest, consider multiple users of information, and consider the concerns of both governmental and non-governmental entities. To date, they have only analyzed the problem. The November 16, 2006, Report of the Program Manager, Information Sharing Environment, indicates that the interagency Information Sharing Council (ISC) created to develop an implementation plan for the ISE, along with standardizing procedures for sensitive but unclassified information, has now created a Coordinating Committee which will submit recommendations for SBU standardization through the White House policy process. We were told that a recommendation would be transmitted to the White House in January 2007, but I am not aware whether this has happened or whether the recommendation will ever be made public.

For my own part, I was impressed with Ambassador McNamara's work to date, but I was not left with any strong impression that a transparent, government-wide information-sharing plan will emerge any time soon. First, there are many steps in the process that do not yet appear to have taken place. A recommendation has yet to be circulated for review by interested parties. Any recommendations should be made available to the public for comment. Even the general outline of a program, which was previewed to me and others in November 2006, raised several concerns about transparency, government accountability, and appropriate procedures. Once a recommendation is accepted, then an implementation plan will be necessary. It is possible that there will need to be statutory or regulatory changes to facilitate implementation. There certainly will be budgetary issues raised by any recommendation and plan for standardization.

Second, the focus of the Program Manager's effort is solely on information related to homeland security, law enforcement and terrorism.   The problem of sensitive unclassified information is far broader, and even the category of information that affects our security is likely more extensive than is covered by the Program Manager's mandate. Placement of the Program Manager at the ODNI further limits the likelihood that a government-wide solution will be considered or emerge as an outgrowth of the process. Because of the placement within the ODNI, the program manager is likely to face great challenges in implementing an information sharing network that includes agencies outside the intelligence community. Issues of information security, information sharing, and public access to information should not be addressed in a piecemeal manner. There are best practices in some agencies that should be shared, as well as lessons to be learned about the costs and benefits of secrecy and disclosure. If the problem of information controls interfering with information sharing is ever to be solved, it will require a government-wide commitment.

Third, there does not appear to be any schedule in place for moving the process forward. The fact that the Program Manager has collected and analyzed scores of information control policies is progress. That analysis surely offers insight into what works and what does not. Now the analysis must be translated into a plan with strict deadlines and funding in order to make implementation a reality. Given that the project has been perpetually behind schedule, there is cause for concern about the development of an actionable plan and implementation.

Unnecessary secrecy has been on the rise since September 11, with the result of threatening our safety and national security while impeding the process of democracy and the effective functioning of government. There is no time for turf wars or bureaucratic inertia. We are long overdue for solving the challenges of information sharing and overcoming the strain on government accountability brought about by excessive secrecy. SBU designations have been noted by government authorities as a major impediment to information sharing, yet no solution to the problem has been developed. I am hopeful that my testimony today offers a rationale and a sense of urgency for instituting stronger measures to encourage needed reforms in information-control programs across the federal government. I am grateful for your interest in these issues and am happy to respond to any questions.

Meredith Fuchs serves as the General Counsel to the non-governmental National Security Archive at George Washington University. At the Archive, she oversees Freedom of Information Act and anti-secrecy litigation, advocates for open government, and frequently lectures on access to government information. She has supervised five government-wide audits of federal agency FOIA performance including: “Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government’s Policies on Sensitive Unclassified Information.” She is the Secretary of the Board of Directors of the American Society of Access Professionals (ASAP), a private professional association of FOIA personnel who serve throughout the federal government. She is the author of “Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy,” 58 Admin. L. Rev. 131 (2006); and “Greasing the Wheels of Justice: Independent Experts in National Security Cases,” 28 Nat’l Sec. L. Rep. 1 (2006).

Previously she was a Partner at the Washington, D.C. law firm Wiley Rein & Fielding LLP, where she was a member of the Litigation, Insurance, Privacy and E-Commerce practice groups. Ms. Fuchs served as a law clerk to the Honorable Patricia M. Wald, U.S. Court of Appeals for the District of Columbia Circuit, and to the Honorable Paul L. Friedman, U. S. District Court for the District of Columbia. She received her B.Sc. (honors) from the London School of Economics and Political Science and her J.D. (cum laude) from the New York University School of Law.