Testimony of Mark D. Agrast

Before the Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
U.S. House of Representatives

Hearing on "Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Information"

June 28, 2007

Testimony of Mark D. Agrast
Senior Fellow, Center for American Progress

Before the Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
U.S. House of Representatives

Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Information

June 28, 2007

Madame Chair, Ranking Member Reichert, and members of the subcommittee, thank you for conducting this hearing and inviting me to testify.

My name is Mark Agrast. I am a Senior Fellow at the Center for American Progress, where I work on issues related to the Constitution, separation of powers, terrorism and civil liberties, and the rule of law.

Before joining the Center, I was an attorney in private practice and spent over a decade on Capitol Hill, most recently as Counsel and Legislative Director to Congressman William D. Delahunt of Massachusetts. A biographical statement is appended to my testimony.

In an address to the Oklahoma Press Association in February 1992, former Director of Central Intelligence, Robert M. Gates, now the Secretary of Defense, noted that the phrase "CIA openness" can seem as much an oxymoron as "government frugality" and "bureaucratic efficiency."

That seeming contradiction in terms illustrates the anomalous role that secrecy plays in a democracy that depends so profoundly on an informed and engaged citizenry.

At the same time, most Americans understand and accept the need to withhold from public view certain national security information whose disclosure poses a genuine risk of harm to the security of the nation.

But the events of 9/11 taught us how dangerously naïve it would be to equate secrecy with security. As the 9/11 Commission concluded, too much secrecy can put our nation at greater risk, hindering oversight, accountability, and information sharing.

Too much secrecy—whether through over-classification or through pseudo-classification—conceals our vulnerabilities until it is too late to correct them.

It slows the development of the scientific and technical knowledge we need to understand threats to our security and respond to them effectively.

It short-circuits public debate, eroding confidence in the actions of the government.

And finally, it undermines the credibility of the classification system itself, encouraging leaks and breeding cynicism about legitimate restrictions. As Associate Justice Potter Stewart famously cautioned in the Pentagon Papers case:

> I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained. [1]

The Commission on Protecting and Reducing Government Secrecy, chaired by Sen. Daniel Patrick Moynihan, reached a similar conclusion in its 1997 report: "The best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall."[2]

Classification, Declassification and Reclassification

The Moynihan Commission was created by Congress to consider whether it was time to rethink the vast system of secrecy that had been brought into being during the Cold War. The Commission recommended a series of statutory reforms to the classification system that were widely praised but never implemented.

The spirit of the Moynihan recommendations can certainly be discerned in the contemporaneous amendments to the classification system that were instituted by President Clinton under Exec. Order No. 12958. The order established a presumption of access, directing that "If there is significant doubt about the need to classify information, it shall not be classified." Similarly, the order provided that "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level." The Clinton order also:

- Limited the duration of classification, providing that where the classifier cannot establish a specific point at which declassification should occur, the material will be declassified after 10 years unless the classification is extended for successive 10-year periods under prescribed procedures.
- Provided for automatic declassification of government records that are more than two years old and have been determined by the Archivist of the United States to

[1] N.Y. Times Co. v. U.S., 403 U.S. 713, 729 (1971) (Stewart, J., concurring).
[2] REPORT OF THE COMM'N ON PROTECTING & REDUCING GOV'T SECRECY (1997) at xxi [hereinafter Moynihan Commission Report].

have permanent historical value, allowing for the continued classification of certain materials under specified procedures.
- Established a balancing test for declassification decisions in "exceptional cases," permitting senior agency officials to exercise discretion to declassify information where "the need to protect such information may be outweighed by the public interest in disclosure of the information."
- Prohibited reclassification of material that had been declassified and released to the public under proper authority.
- Authorized agency employees to bring challenges to the classification status of information they believe to be improperly classified.
- Created an Interagency Security Classification Appeals Panel (ISCAP) to adjudicate challenges to classification and requests for mandatory declassification, and to review decisions to exempt information from automatic declassification.

The changes instituted by President Clinton were largely erased by his successor, who issued a revised executive order in 2003. Exec. Order No. 13292 eliminated the presumption of access, leaving officials free to classify information in cases of "significant doubt." It also:

- Relaxed the limitations on the duration of classification, and made it easier for the period to be extended for unlimited periods.
- Postponed the automatic declassification of protected records 25 or more years old from April 2003 to December 2006, and reduced the showing that agencies must make to exempt historical records from automatic declassification.
- Revived the ability of agency heads to reclassify previously declassified information if the information "may reasonably be recovered."
- Allowed the Director of Central Intelligence to override decisions by ISCAP, subject only to presidential review.

The results of this shift in policy are reflected in the annual classification statistics published by the Information Security Oversight Office (ISOO). The number of classification actions by the government hit an all-time high of 15.6 million in 2004, with only slightly fewer (14.2 million) reported in 2005. This was nearly twice the number of classification actions (8.6 million) taken in 2001, the first year of the Bush administration, and three times the number (5.8 million) taken in 1996, the last year of President Clinton's second term.[3]

As classification actions have soared, declassification actions have plummeted. President Clinton oversaw the declassification of more historic materials than all previous presidents combined. During his last six years in office, 864 million pages were declassified, hitting an all-time high of 204 million pages in 1997 alone. Under the Bush administration, the numbers have fallen precipitously. Only 245 million pages were

[3] INFO. SEC. OVERSIGHT OFFICE, NAT'L ARCHIVES & RECORDS ADMIN., REPORT TO THE PRESIDENT 2005 at 13.

declassified from 2001-2005, with fewer than 30 million pages were declassified in 2005.[4]

Apart from its costs to both openness and security, all this classifying and declassifying comes at a heavy financial cost as well. In 2005, the cost of securing classified information was $7.7 billion, of which only $57 million was spent on declassification. In all, for every dollar the federal government spent to release old secrets, it spent $134 to create new ones.[5]

What the numbers cannot reveal is whether classification decisions are lawful and appropriate. Estimates of the extent of over-classification vary, but I was particularly struck by Mr. Leonard's testimony before this subcommittee last March, in which he said that an audit conducted by the Information Security Oversight Office found that even trained classifiers, armed with the most up-to-date guidance, "got it clearly right only 64 percent of the time."[6]

There are also instances in which over-classification is the result, not of honest error, but of a desire to conceal. Both the Clinton and Bush executive orders prohibit the use of the classification system to "conceal violations of law, inefficiency, or administrative error" or "prevent embarrassment to a person, organization, or agency." Yet at least some recent classification decisions could have had little purpose other than to suppress information that might be embarrassing to the government.

A particularly troubling example is the decision by the Department of Defense to classify in its entirety the March 2004 report of the investigation by Maj. Gen. Antonio M. Taguba of alleged abuse of prisoners by members of the 800th Military Police Brigade at Baghdad's Abu Ghraib Prison. According to an investigation by the Minority Staff of the House Committee on Government Reform:

> One reporter who had reviewed a widely disseminated copy of the report raised the issue in a Defense Department briefing with General Peter Pace, the Vice Chairman of the Joint Chiefs of Staff, and Secretary Rumsfeld. The reporter noted that 'there's clearly nothing in there that's inherently secret, such as intelligence sources and methods or troop movements' and asked: 'Was this kept secret because it would be embarrassing to the world, particularly the Arab world?' General Pace responded that he did not know why the document was marked secret. When asked whether he could say why the report was classified, Secretary Rumsfeld answered: 'No, you'd have to ask the classifier.'[7]

[4] Id. at 15.
[5] OPENTHEGOVERNMENT.ORG, SECRECY REPORT CARD 2006 at 4.
[6] *Overclassification and Pseudo-classification: The Impact on Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Comm. on Homeland Sec.*, 110th Cong. (2007) (statement of J. William Leonard).
[7] MINORITY STAFF OF HOUSE COMM. ON THE JUDICIARY, 10TH CONG., REPORT ON SECRECY IN THE BUSH ADMINISTRATION (2004) at 50.

The desire to prevent embarrassment seems also to have played a role in the Bush administration's aggressive reclassification campaign. According to a February 2006 report by the National Security Archive, the administration has reclassified and withdrawn from public access 9,500 documents totaling 55,500 pages, including some that are over 50 years old. For example:

- A complaint from the Director of Central Intelligence to the State Department about the bad publicity the CIA was receiving after its failure to predict anti-American riots in Colombia in 1948.
- A document regarding an unsanctioned CIA psychological warfare program to drop propaganda leaflets into Eastern Europe by hot air balloon that was canceled after the State Department objected to the program.
- A document from spring 1949, revealing that the U.S. intelligence community's knowledge of Soviet nuclear weapons research and development activities was so poor that America and Britain were completely surprised when the Russians exploded their first atomic bomb six months later.
- A 1950 intelligence estimate, written only 12 days before Chinese forces entered Korea, predicting that Chinese intervention in the conflict was "not probable."[8]

These reclassification actions call to mind the observations of the late Erwin N. Griswold, former Solicitor General of the United States and Dean of Harvard Law School, who argued the Pentagon Papers case before the Supreme Court in 1971. Presenting the case for the government, he had argued that the release of the Pentagon Papers would gravely damage the national security. Nearly two decades later, Griswold reflected on the lessons of that case:

> It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past. This is the lesson of the Pentagon Papers experience, and it may be relevant now.[9]

Pseudo-Classification

For all its faults, the classification system has many virtues as well. Classification actions are subject to uniform legal standards pursuant to executive order. These actions can be taken by a limited number of officials who receive training in the standards to be applied;

[8] MATTHEW M. AID, NAT'L SEC. ARCHIVE, DECLASSIFICATION IN REVERSE: THE U.S. INTELLIGENCE CMTY'S SECRET HISTORICAL DOCUMENT RECLASSIFICATION PROGRAM (2006).

[9] Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information,* WASH. POST, Feb. 15, 1989, at A25.

they are of limited duration and extent; they are monitored by a federal oversight office; they can be challenged; and they can be appealed.

The same cannot be said for the potpourri of unclassified control markings used by federal agencies to manage access to sensitive government information, most of which are defined by neither statute nor executive order, and which collectively have come to be known pejoratively as the "pseudo-classification" system.

Among the better known are Sensitive But Unclassified (SBU), Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI), Critical Infrastructure Information (CII), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO).

While some of these control markings are authorized by statute,[10] others have been conjured out of thin air. Some of these pseudo-classification regimes allow virtually any agency employee (and often private contractors) to withhold information without justification or review, without any time limit, and with few, if any, internal controls to ensure that the markings are not misapplied.

A March 2006 report by the Government Accountability Office (GAO) found that the 26 federal agencies surveyed use 56 different information control markings (16 of which belong to one agency) to protect sensitive unclassified national security information. The GAO also found that the agencies use widely divergent definitions of the same controls.[11]

According to the GAO report, the Department of Homeland Security (DHS) employs five of these control markings: For Official Use Only (FOUO) (agency-wide); Law Enforcement Sensitive (LES) (agency-wide); Limited Official Use (LOU) (U.S. Secret Service); Protected Critical Infrastructure Information (PCII) (Directorate for Preparedness); and Sensitive Security Information (SSI) (Transportation Security Administration and U.S. Coast Guard).

The department's approach to the use of these designations is set forth in a DHS management directive regarding the treatment of sensitive but unclassified information originating within the agency.[12] The directive is chiefly concerned with the For Official Use Only designation, which it says will be used "to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation." The directive identifies 11 categories of SBU information that can be designated as FOUO, and provides that the designation can be

[10] *See, e.g.*, Aviation and Transp. Sec. Act, Pub. L. No. 107-71; Fed. Info. Sec. Act, Pub. L. No. 107-347; Homeland Sec. Act, Pub. L. No. 107-296; Critical Infrastructure Info. Act, Pub. L. No. 107-296.
[11] U.S. GOV'T ACCOUNTABILITY OFFICE, REP. NO. GAO-06-385, INFORMATION SHARING: THE FEDERAL GOVERNMENT NEEDS TO ESTABLISH POLICIES AND PROCESSES FOR SHARING TERRORISM-RELATED AND SENSITIVE BUT UNCLASSIFIED INFORMATION (2006).
[12] Safeguarding Sensitive But Unclassified (For Official Use Only) Information, Mgt. Dir. No. 11042 (2004), *at* http://www.fas.org/sgp/othergov/dhs-sbu.html, *revised by* Mgt. Dir. No. 11042.1, (2005), *at* http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf [hereinafter Safeguarding].

made by any DHS employee, detailee, or contractor and will remain in effect indefinitely until the originator or a management official determines otherwise.

For good measure, the directive notes that where other agencies and international organizations use similar terminology but apply different requirements to the safeguarding of the information, the information should be treated in accordance with whichever requirements are the more restrictive.

A 2004 report by the JASON Program Office at MITRE Corporation suggests that the designation authorities at DHS are not atypical: "'Sensitive but unclassified' data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used."[13]

As in the case of classification and reclassification actions, these designations have at times been used not to protect legitimate national security secrets, but to spare the government from embarrassment. In a March 2005 letter to Rep. Christopher Shays, then the Chairman of the House Committee on Government Reform, Rep. Henry Waxman cited examples in which:

- The State Department withheld unclassified conclusions by the agency's Inspector General that the CIA was involved in preparing a grossly inaccurate global terrorism report.
- The State Department concealed unclassified information about the role of John Bolton, Under Secretary of State for Arms Control, in the creation of a fact sheet that falsely claimed that Iraq sought uranium from Niger.
- The Department of Homeland Security concealed the unclassified identity and contact information of a newly appointed TSA ombudsman whose responsibility it was to interact daily with members of the public regarding airport security measures.
- The CIA intervened to block the chief U.S. weapons inspector Charles A. Duelfer, from revealing the unclassified identities of U.S. companies that conducted business with Saddam Hussein under the Oil for Food program.
- The Nuclear Regulatory Commission sought to prevent a nongovernmental watchdog group from making public criticisms of its nuclear power plant security efforts based on unclassified sources.[14]

In another case, currently in litigation, a federal air marshal blew the whistle when TSA attempted to reduce security on "high risk" flights, and the agency allegedly retaliated by retroactively designating the material he had disclosed as Sensitive Security Information (SSI).[15]

---

[13] JASON PROGRAM OFFICE, MITRE CORPORATION, HORIZONTAL INTEGRATION: BROADER ACCESS MODELS FOR REALIZING INFORMATION DOMINANCE 5 (2004).
[14] H.R. Rep. No. 109-18, at 16 (2005) (letter from Henry Waxman to Christopher Shays).
[15] PROJECT ON GOV'T OVERSIGHT, ALERT: ROBERT MACLEAN V. DHS (2007), *at* http://pogo.org/p/government/rmaclean-dhs.html

Another concern arises out of the interplay between unclassified control markings and the Freedom of Information Act (FOIA). Certain unclassified control markings, including Sensitive Security Information (SSI) and Critical Infrastructure Information (CII), are specifically exempt by statute from release under FOIA. But some agencies have claimed that other unclassified control markings constitute an independent legal basis for exempting information from public disclosure under FOIA—even in the absence of an express statutory exemption and even where the information does not fit within an existing exemption.

Such claims prompted the American Bar Association's House of Delegates to adopt a resolution in February 2006 urging the Attorney General to clarify that such designations should not be used to withhold from the public information that is not authorized to be withheld by statute or executive order.

As it happens, the DHS directive meets the ABA standard. It provides that FOUO information is not automatically exempt from disclosure under FOIA and that FOUO information may be shared with other agencies and government entities "provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity."[16]

But whether or not an agency has a legal basis for withholding pseudo-classified information not otherwise exempt under FOIA is almost beside the point. The designation is itself sufficient to exert a chilling effect on FOIA disclosures. As Thomas S. Blanton of the National Security Archive testified before a subcommittee of the House Committee on Government Reform in March 2005, "the new secrecy stamps tell government bureaucrats 'don't risk it'; in every case, the new labels signal 'find a reason to withhold.'"[17]

An article published in the Washington Post on June 24, 2007, brought to light a pseudo-classification scheme apparently invented by the Vice President of the United States. His office has been giving reporters documents labeled: "Treated As: Top Secret/SCI"—an apparent attempt to treat unclassified material as though it were Sensitive Compartmented Information (SCI)—a special access designation reserved for secrets whose disclosure would cause 'exceptionally grave damage to national security.'"[18]

Unlike the Cheney innovation, Special Access Programs (SAPs), which limit access above and beyond the three-tiered classification system, are authorized by law, and are confined to a relatively limited circle of senior officials. Exec. Order No. 12859, as amended, provides that unless otherwise authorized by the President, only certain named

[16] Safeguarding, *supra* note 11.
[17] *Emerging Threats: Over-classification and Pseudo-classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats and Int'l Relations of the House Comm. on Gov't Reform*, 109th Cong. (2005) (statement of Thomas S. Blanton).
[18] Barton Gellman & Jo Becker, *A Different Understanding with the President*, WASH. POST, June 24, 2007, at A1.

officials are authorized to establish such programs. The list includes the Secretaries of State, Defense, and Energy, and the DCI, or the principal deputy of each. Interestingly, the list does not include the Vice President—perhaps in anticipation of his novel assertion that the Office of the Vice President is not an agency of the Executive Branch and need not comply with the requirement under Exec. Order 12859 that such agencies file an annual report with ISOO.[19]

The fact that SAPs are authorized by executive order does not mean they are immune from the deficiencies of pseudo-classifications. The Moynihan Commission noted a "lack of standardized security procedures" that "contributes to high costs and other difficulties," and recommended the establishment of a single set of security standards for Special Access Programs—another of its sensible recommendations which, as far as is known, has not been carried out.[20]

Recommendations for Congress

Madame Chair, you and the subcommittee should be commended for exercising your oversight authority over the treatment of national security information—both classified and unclassified—at the Department of Homeland Security. Such scrutiny is essential, and it is long overdue.

I would also respectfully suggest that the time has come for the committee, and for Congress, to exercise its *legislative* authority over these matters. For 67 years, Congress has largely ceded that authority to the president, and as I hope I have explained, the results have been decidedly mixed.

It has been ten years since the Moynihan Commission urged Congress to legislate the rules that protect national security information, rather than leaving it up to the executive branch to police itself. It is time for Congress to take up that challenge.

A. Systemic solutions

Many of the problems facing the classification system are systemic, and they require comprehensive, government-wide solutions. Among other things, Congress should reinstate the provisions of Exec. Order No. 12958 which (a) established a presumption against classification in cases of significant doubt (a policy which the Moynihan Commission urged Congress to codify); (b) permitted senior agency officials to exercise discretion to declassify information in exceptional cases where the need to protect the information is outweighed by the public interest in disclosure; and (c) prohibited reclassification of material that had been declassified and released to the public under proper authority.

[19] Peter Baker, Cheney Defiant on Classified Material: Executive Order Ignored Since 2003, WASH. POST, June 22, 2007, at A1.
[20] MOYNIHAN COMMISSION REPORT at 28.

Congress also should undertake a thorough and comprehensive examination of the growing use of agency control markings to restrict access to unclassified information. Much has been said, and rightly so, about the importance of information sharing among government agencies. But what is the justification for a system that entrusts low-level employees and private contractors with the non-reviewable discretion to determine whether an unclassified document—a document that doesn't even rate a "Confidential" stamp—a document that may not even qualify for a FOIA exemption—is too sensitive for public view?

Before Congress acquiesces in the further proliferation of these designations, it should consider whether those that already exist place an unwarranted burden on the free exchange of information, not only among government officials, but between the government and the people who elect it.

At a minimum, Congress should prohibit agencies from adopting unclassified controls that are not expressly authorized by statute (or executive order), and should mandate strict standards for any controls it does authorize to minimize their impact on public access.

H.R. 5112, the Executive Branch Reform Act, which was reported by the House Government Reform Committee during the 109th Congress, directs the Archivist of the United States to promulgate regulations banning the use of information control designations not defined by statute or executive order. If the Archivist determines that there is a need for some agencies to use such designations "to safeguard information prior to review for disclosure," the regulations shall establish standards designed to minimize restrictions on public access to information. The regulations shall be the sole authority for the use of such designations, other than authority granted by statute or executive order.

This approach would ameliorate some of the worst features of what is today an unregulated wilderness of inconsistent standards and insufficient checks. But it begs the question of whether Congress should be authorizing agency officials to withhold unclassified information in the first place. Such powers are all too easily given, and once they are in place, it is virtually impossible to get rid of them.

I hope that Congress will consider codifying standards that incorporate these policies. But there are also many steps that can be taken to reform the management of national security information one department at a time. By undertaking such reforms at the Department of Homeland Security—by making DHS the "gold standard"—Congress can create a model for best practices that other agencies can adopt.

B. <u>The Classification System at DHS</u>

(1) Congress should establish an Information Security Oversight Office, modeled after the Information Security Oversight Office at the National Archives and Records Administration, to oversee security classification programs at DHS. Its responsibilities would include development of implementing directives and

instructions; maintenance of liaison with ISOO and agency counterparts; monitoring of agency compliance and preparation of reports to Congress; and development of security classification education and training programs.

(2) Congress should establish an independent DHS Classification Review Board to ensure that information is declassified as soon as it no longer meets the criteria for classification. Among the responsibilities of the board would be to facilitate and review requests for declassification and classification challenges, and to conduct an independent ongoing review of classified materials to determine whether they are properly classified.

(3) Congress should establish an independent ombuds office within DHS to provide assistance with classification challenges and requests for declassification.

(4) Congress should require the DHS Inspector General to conduct periodic audits of the DHS classification program and report to Congress on the appropriateness of classification decisions.

(5) Congress should require DHS to implement a system of certification for DHS officials with classification authority and to provide them with training in proper classification practices.

C. <u>Sensitive Information Controls at DHS</u>

As noted above, I hope that Congress will reconsider the question of whether agency employees and private contractors should be given a license to withhold unclassified, non-FOIA exempt information from the public. But short of curtailing the use of unclassified control markings, there are steps that can be taken by DHS to minimize error and abuse, and reduce the impact of pseudo-classification on public access to information.

(1) Congress should require DHS to place strict limits on the number of agency officials authorized to designate FOUO and other unclassified information as controlled, to implement a system of certification for DHS officials with designation authority, and to provide authorized officials with training in proper designation practices.
(2) Congress should require DHS to limit the duration of controls on unclassified information and provide procedures by which such controls can be removed.
(3) Congress should require DHS to develop procedures by which members of the public can challenge unclassified designations.
(4) Congress should require the DHS Inspector General to conduct periodic audits of the use of controls on unclassified information and report to Congress on the appropriateness of designations.
(5) The Homeland Security Committee should oversee DHS implementation of—
    a. The directives regarding the use of the SSI designation by TSA which Congress included in the DHS Appropriations Bill for FY 2007 (Pub. L.

109-295). Those directives require review of any document designated SSI whose release is requested and require release of certain documents designated SSI after three years unless the DHS Secretary provides an explanation as to why it should not be released.

b. The recommendations included in the GAO report of June 2005 evaluating the use of the SSI designation by TSA.[21] The GAO found significant deficiencies in TSA's management of SSI, and recommended that the Secretary of DHS direct the TSA Administrator to:
    i. Establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI.
    ii. Establish clear responsibility for the identification and designation of information that warrants SSI protection.
    iii. Establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA.
    iv. Establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.

Conclusion

By helping to ensure that the government keeps secret only the information that needs to be secret, these measures would enhance both openness and security—at DHS and throughout the government.

Thank you.

[21] U.S. GOV'T ACCOUNTABILITY OFFICE, REP. NO. GAO-05-677 TRANSPORTATION SECURITY ADMINISTRATION: CLEAR POLICIES AND OVERSIGHT NEEDED FOR DESIGNATION OF SENSITIVE SECURITY INFORMATION (2005).