

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

MEMORANDUM

To: Members of the Subcommittee on National Security,
Emerging Threats, and International Relations

From: Lawrence J. Halloran

Subject: Briefing Memorandum for the hearing, *Too Many Secrets:
Overclassification as a Barrier to Critical Information Sharing*,
scheduled for Tuesday, August 24, 10 a.m., 2154 Rayburn
House Office Building.

Date: August 17, 2004

PURPOSE OF THE HEARING

The purpose of the hearing is to examine the impact of excessive classification and delayed declassification of federal materials on 9/11 Commission recommendations for more effective information sharing.

HEARING ISSUES

1. **To what extent do current policies and practices permit the excessive or abusive classification, or delayed declassification, of federal materials?**
2. **What is the impact of current classification policies and practices on efforts to enhance interagency and intergovernmental information sharing?**

BACKGROUND

The Final Report of the National Commission on Terrorist Attacks Upon the United States (“the 9/11 Commission Report”) found that information security policies and practices impede the robust forms of information sharing required to meet the threat of terrorism. The Report states:

Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency’s incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though this costs— even in literal financial terms— are substantial. There are no punishments for *not* sharing information. Agencies uphold a “need-to-know” culture of information protection rather than promoting a “need-to-share” culture of integration. (*9/11 Commission Report at p. 417*)

The Commission endorsed creation of a decentralized, technologically advanced “trusted information network” to make threat information more widely accessible and to reverse Cold War paradigms and cultural biases against information sharing. The Commission noted such a network had been described in a task force report commissioned by the Markle Foundation (**Web Resources 1**), but

the concept "has not yet been converted into action." (9/11 Commission Report at p. 418.)

Since 1940, classification of official secrets has been governed by policies and procedures flowing from executive orders of the President. Current security requirements are mandated by E.O. 12958 as amended by E.O. 13292. **(Attachment 1)** Successive executive directives reflect Cold War counterespionage concerns as well as persistent tension between the need for secrecy the public access to government information. By varying degrees, Presidents sought to protect national secrets through broader or narrower delegation of classification authority, by expanding or contracting categories of classifiable information and by endorsing or opposing the use of automatic declassification deadlines.

The first post-Cold War policy on classification was issued by President Clinton in 1995. E.O. 12356 reset previous default settings, directing classifiers *not* to shield information of doubtful value and to classify information at the *lowest* rather than the highest possible level. With some exceptions, the order sets a ten year limit on classification markings and provides broadened opportunities for declassification of official materials. Reclassification is prohibited if the material has otherwise been properly put in the public domain. A new Interagency Security Classification Appeals Panel was established to make final decisions on certain classification challenges and declassification exemptions. **(Attachment 1, p5)** President Bush issued E.O. 13292, amending E.O. 12958, that reverts to a "when in doubt, classify" standard, expands classification authorities and categories and postponed automatic declassification of some records.

Security concerns after the September 11th attacks prompted some departments and agencies to increase the type and volume of information shielded from public view by *Confidential*, *Secret* or *Top Secret* markings. But executive classification of significant portions of congressional investigative reports revived the debate over the objectivity of information security standards and the potential for

excessive, abusive or politically motivated classification.

(Attachment 2) Some have called for appointment of an independent panel to review and settle disputes over classification and declassification. **(Attachment 2, p. 2; H.R. 4855 and S. 2672)**

The Information Security Oversight Office (ISOO) within the National Archives and Records Administration is responsible for executive branch oversight of security classification matters. The ISOO 2003 Report to the President noted that 3,978 separate offices or individuals made 238,030 classification decisions in FY03 affecting more than 14 million documents. Agencies reported an eight percent increase in original classifications over the previous year, with most of the increase attributable to the Departments of Defense and Justice. **(Web Resources 2)**

The report acknowledged that, "many senior officials will candidly acknowledge that the government classifies too much information, although oftentimes the observation is made with respect to the activities of agencies other than their own. The potential use of excessive classification is supported, in part, by agency input indicating that overall classification activity is up over the past several years." The report goes on to note the inevitable tendency to protect more information in times of war but notes the easy propensity to "err on the side of caution" concedes more error than a balanced system should tolerate, concluding that, "Too much classification unnecessarily impedes effective information sharing."

DISCUSSION OF HEARING ISSUES

1. To what extent do current policies and practices permit the excessive or abusive classification, or delayed declassification, of federal materials?

Most concede it is impossible to quantify the extent of overclassification, noting it is difficult enough to determine how much information remains classified at any given time. The problem of assessing the true scope of what is classified or overclassified is compounded by the proliferation of information media. One classification decision may affect one page, one thousand pages, or one thousand computer discs each containing one thousand pages.

According to a 1997 report, "Given this uncertainty, it should not be surprising that there is little agreement on the extent of overclassification. For over a decade the ISOO has estimated that between one and ten percent of all classified documents are unnecessarily classified. In 1995, a White Paper prepared by the DoD Inspector General concluded that the classification process at the DoD is "fundamentally sound" and that "the present size of classified holdings is not the result of too much information being needlessly classified." In contrast, a 1985 preliminary study prepared by the staff of two House subcommittees proposed a classification system in which "roughly nine-tenths of what is now classified" would no longer qualify for classification. More recently, former NSC Executive Secretary Rodney B. McDaniel estimated that only ten percent of classification was for "legitimate protection of secrets." Given the uncertainty surrounding the breadth of classification, however, efforts to quantify with any precision the extent of unnecessary classification not only may be futile, but are unlikely to help in understanding its causes or possible remedies." **(Web Resources 3)**

The report further noted that despite being required to mark documents to indicate which portions are classified and which are not, employees in some agencies continue to mark materials "Entire Text

Classified," increasing the difficulty of distinguishing which parts truly need protection and which might later be declassified.

The creation of classification safe harbors, or sacred cows, also contributes to the volume of information put into those categories and the set of documents that often remain beyond declassification review. Intelligence sources and methods, personnel levels and budgets have become classification icons into which very remotely related information can be secreted. The Cold War nuclear doctrine of "born classified, always classified" also encourages overclassification.

(Web Resources 4)

Over-classification is viewed by some as an inevitable political and cultural bureaucratic response to an exclusive "need to know" security standard. Such an environment breeds what has been called "the cult of classification" whose members have every incentive to increase their own importance by increasing the volume of information only they can see. **(Attachment 3)**

2. What is the impact of current classification policies and practices on efforts to enhance interagency and intergovernmental information sharing?

A far more horizontal world - characterized by transnational terrorism and the need to respond using multinational military coalitions – challenges Cold War paradigms and policies designed to protect official secrets in vertical organizational structures. The 9/11 Commission concluded that inability to integrate the intelligence in hand – both classified and unclassified – across agency lines contributed to the failure to detect or deter the attacks.

Overclassification makes integration of federal agency watch lists and other data bases more complex and more expensive given the need to maintain separate systems and protocols for secure information.

Classified information is also more difficult to include in alerts to state and local officials since many do not have required clearances and cannot justify committing to costly responsive actions based only on scrubbed, generic information. In testimony before the Government Reform Committee on August 3, Comptroller General David Walker noted that the federal government did not generally consider the role of state and local officials in national security matters but that September 11th and the continuing threat of terrorism create a compelling "need to share" intelligence information at that level. **(Web Resources 5)**

In 1970, the Defense Science Board concluded that overclassification also undermines the credibility of government security decisions. **(Web Resource 4, Note 2)** Indiscriminate and excessive classification also tends to mask the volume and utility of information now available from open sources.

Overclassification ultimately incurs avoidable fiscal costs and compromises national security. Adversarial, versus automatic, declassification procedures are cumbersome and time consuming. Safeguards for voluminous classified material require costly security measures. And government officials confronted with dizzyingly complex rules for numerous categories of classified information often cannot or do not distinguish truly significant security matters from routine material market secret out of an excess of caution or zeal. It is often observed in this regard "he who defends everything defends nothing."

ATTACHMENTS

1. CRS Report, *Security Classification Policy and Procedures: E.O. 12958, as Amended*, 97-771, May 14, 2003.
2. CRS Report, *Secrecy Versus Openness: Arrangements for Balancing Competing Needs*, RS21895, August 4, 2004.
3. "I Could Tell You, But I'd Have to Kill You: The Cult of Classification in Intelligence," STRATFOR Analysis, September 18, 2000.

WEB RESOURCES

1. http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf
2. http://www.archives.gov/isoo/reports/2003_annual_report.html
3. <http://www.fas.org//sgp/library/moynihan/>
4. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/index.htm>
5. <http://reform.house.gov/UploadedFiles/GAO%20-%20Walker%209-11%20Testimony.pdf>