Hearing of the

United States House of Representatives

Committee on Homeland Security

Subcommittee on Intelligence, Information Sharing and

Terrorism Risk Assessment

Over-Classification and Pseudo-Classification:

Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information.

Thursday, June 28, 2007

Testimony of Suzanne E. Spaulding

Chairwoman Harman, Ranking Member Reichert, and members of the Committee, thank you for this opportunity to testify today about classification issues at the Department of Homeland Security. This is an important issue and I commend the committee for making it a priority.

I was fortunate enough to spend 20 years working national security issues for the government, including 6 years at CIA and time at both the Senate and House Intelligence Committees. I have seen first hand how important it is to get the classification issue right.

It may seem counterintuitive to some, but avoiding over-classification is essential to protecting vital national security secrets. Those handling classified documents will have greater respect for that "Top Secret" stamp if they know that things are only classified when their disclosure would truly harm national security. When things are classified whose disclosure clearly would not harm national security, it tempts some individuals to believe that they can decide what is really sensitive and what is not. This could apply to employees in the intelligence community or others, such as members of the media, who receive classified documents. In making this observation, I certainly do not mean in

any way to excuse the disclosure of classified information, merely to note that the risk of leaks is heightened by over-classification.

A similar phenomenon follows the increasingly common practice of "selective declassification" by government officials. This selective declassification can be accomplished either by unofficial leaks to the media or by official decisions to declassify material. Strategic and carefully considered decisions to make previously classified information available to the public can be an important and effective way of increasing the transparency that is so vital for a functioning democracy. However, when the disclosures appear to be designed to advance a particular political agenda or to gain advantage in a policy dispute, it again undermines the respect for and confidence in the classification system. An employee or reporter who sees senior officials deciding that classification isn't as important as their particular agenda may be emboldened to make similar decisions. This risk is heightened when the classification is done selectively so as to reveal only intelligence that supports one side of the issue, while leaving contrary intelligence classified.

Just as getting the classification process right is vital for protecting true secrets, it is essential that information that can be shared without jeopardizing national security is not prevented by over-classification from getting to those who could make use of it. As the 9/11 Commission Report made clear, this is particularly urgent for our counterterrorism efforts.

It is appropriate that the Committee has decided to begin with an effort to make the Department of Homeland Security the "Gold Standard" for reducing over-classification, since DHS faces the most significant imperative to provide relevant information to, and receive and analyze information from, a wide range of users who are not traditional members of the national security community. Key players at the state and local level, in the private sector, and within DHS' own entities, are unlikely to have clearances. Yet they serve vital roles in protecting the homeland and can provide, benefit from, and help analysts to better understand, information that is gathered overseas and in the US. If this information is unnecessarily restricted, it threatens homeland security by hampering the ability of these key players to contribute to the mission.

I know that the committee is considering a number of ideas, including a certification process to ensure that those who have authority to classify documents are properly trained to recognize when information is truly sensitive and regular audits of existing classified documents to assess the scope and nature of any over-classification. I think these are sound suggestions. There are additional near-term and longer-term steps that the Committee might also consider.

1. ***Require that documents be written in unclassified version first, to the maximum extent possible.*** Traditional practice in the intelligence community has been to prepare a classified document reflecting the intelligence and then, if dissemination to non-cleared individuals was required, to prepare an unclassified version at the bottom of the document after a "tear line." These are known as "tear sheets;" the recipient would tear off the bottom portion to provide to the un-cleared recipient. Instead, to facilitate the admonition to move from a "need to know" to a "need to share" culture --what the Markle Foundation called a "culture of distribution"--why not set up the system so that no classified document can be prepared without first entering information in the unclassified section at the top of the document. There may be times when almost nothing can be put it the unclassified portion, but the exercise could prompt more careful effort to distinguish between truly classified information and that which can be shared more broadly. And putting the unclassified version at the top visually reinforces the shift in priorities.

2. ***Enforce "portion marking."*** It used to be standard practice that each paragraph of a document had to be individually determined and marked as classified or unclassified. This requires more careful consideration of what information is actually sensitive and assists in any later efforts to provide an unclassified version of the document. My sense is that, over time, documents are increasingly classified in their entirety, with no portion marking, making it far more difficult and cumbersome to "sanitize" the information for wider dissemination. A simple immediate step would be to enforce the requirement for portion marking for every classified document.

3***. Use technology to tag information as it moves through the system.*** The optimum system would provide even greater granularity than the paragraph portion marking, indicating what precise bits of information are classified. These classification "tags"--perhaps imbedded in metadata-- would then move with the information as it flows through the system and facilitate the preparation of unclassified versions of documents. The more precisely we can isolate truly sensitive information, the easier it will be to identify and disseminate unclassified information.

4. ***Reverse the "default" incentive to over-classify***. Virtually all of the incentives today are in favor of over-classification. The danger of not classifying information that is indeed damaging to national security is well understood. What is not as widely appreciated in the national security risk of over-classification. Thus, there are effectively no penalties in the system for an individual decision to classify unnecessarily. This will not change until performance evaluations consider classification issues. Regular audits can provide insight into individual patterns as well as overall agency performance, for example. Employees who routinely over -classify should be held accountable and receive additional training. And employees should be rewarded for producing reports that can be widely disseminated. In addition,

the system should make it easy to produce unclassified documents and require a bit more effort to classify something. Requiring that unclassified documents be written first and enforcing the requirement for portion marking are some examples. Requiring that the specific harm to national security be articulated in each case might be another possibility, although it is important not too make the system so cumbersome that it undermines the ability to be quick and agile when necessary. Ultimately, you want a process that makes it harder to go around the system that to use it.

5. ***Identify key federal, state, and local officials who can receive relevant classified information by virtue of their office rather than having to get a clearance***. This is how it has always worked with Members of Congress. More recently, this was adopted as the policy for governors. DHS should consider extending this to other key officials.

6. ***Develop innovative ways of sharing information without handing over documents.*** Ultimately, the key is to enhance understanding and knowledge. Too much emphasis is sometimes placed on sharing documents, rather than on sharing ideas, questions, and insights gleaned from those documents. This can often be done without revealing the sensitive information in the documents. In addition, when dealing with unclassified but sensitive information, such as business proprietary information, DHS could consider "partnership panels" where the government and business would come together in a neutral space, share information such as vulnerability assessments and threat information, so as to enhance mutual understanding and benefit from each other's insights, but then leave the space without having handed over the documents.

These are just a few ideas based on practical experience working in classified environments for nearly two decades. I know that the Committee is aware of the outstanding work by the Markle Foundation and others in developing recommendations for improving information sharing and will take those under consideration as well.

The problem of over-classification is an enduring one and presents a daunting challenge. This Committee is to be commended for taking up that challenge and endeavoring to set a new standard at DHS. I appreciate the opportunity to contribute to that important effort. .