Subcommittee on National Security, Emerging Threats, and International Relations
House Committee on Government Reform
August 24, 2004

Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing

Testimony of Bill Crowell
Markle Taskforce on National Security in the Information Age

Good morning Chairman Shays and members of the Subcommittee. I would like to thank you for the opportunity to testify this morning on the recommendations made by the Markle Foundation Task Force on National Security in the Information Age.

Information, and information sharing, are key to fighting terrorism and enhancing our security. Today, our government still does not have all of the information it needs to fight terrorism. And the information it does have is sometimes isolated in different agencies and therefore it is more difficult to see its significance. While the discussion about how to implement the 9/11 Commission's recommendation to restructure the intelligence community is important, another key 9/11 Commission recommendation, creating and implementing a "trusted information network" to facilitate better information sharing among our intelligence and law enforcement organizations at the Federal, State and Local levels could make America safer today.

Towards that end the 9/11 Commission embraced the recommendations for creation of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network made last December by the Markle Foundation Task Force on National Security in the Information Age. The Markle Foundation Task Force consists of leading national security experts from four administrations, as well as widely recognized experts on technology and civil liberties.

The SHARE Network represents a "virtual reorganization" of government by fundamentally altering how people in the many organizations tasked with fighting terrorism share information to facilitate better, faster decision-making. Such an approach, when paired with strong guidelines that govern the system, is also the best way to protect privacy and civil liberties.

The SHARE Network is aimed at moving us from our current need-to-know system into a need-to-share culture.

However, one of the barriers to enabling that move involves classification and information security.

Decisions about sharing intelligence in the government today are still made largely in the context of a system of classification that was developed during the Cold War. During the Cold War, the use of information was dominated by a culture of classification and tight limitations on access, in which information was shared only on a "need to know" basis.

The current system assumes that it is possible to determine in advance who needs to know particular information, and that the risks associated with disclosure are greater than the potential benefits of wider information sharing.

The result of the incentives in place to protect information results in far more information being classified initially—and remaining classified—than is necessary or appropriate.

Another problem with the current system is that each agency has its own classification practices, which leads to cultural tensions when agencies attempt to share information with each other. Government agencies currently rely on processes for "sanitizing" classified information so that it can be shared with other agencies. Some federal agencies sanitize some reports to remove source and method information. But the sanitized version is often still classified, and is usually designed for dissemination only to other federal agencies. Sanitization does not generally occur as a matter of course for many agencies, and no agency, to our knowledge, regularly produces a sanitized version of information that is unclassified and appropriate for wide-scale dissemination to state, local, and private sector entities. The sanitization process is also often slow and cumbersome.

This Cold War mind-set of classification, sanitizing and tight limits on sharing information is ill suited to today's homeland security challenge. While certain information must be protected against unauthorized disclosure, the general mind-set should be one that strives for broad sharing of information with all of the relevant players in the network. The system should be designed to address the enormous difficulty of discovering terrorist plans before they are executed and the needs of the analysts that must uncover these plans, balance against the security concerns on the sources and methods of the collectors. Or, as the 9/11 Commission noted in their report, "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."

The Markle Task Force Approach: New Concepts of Operations and New Technology

The SHARE Network is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants in the system. Such an approach empowers all participants, from local law enforcement officers to senior policy makers. Our approach combines policy and technical solutions to create a network that would substantially improve our ability to predict and prevent terrorist attacks.

WRITE TO SHARE

The SHARE Network is based on the "write to share" concept and moves us from a system based on classification to one based on authorization. By taking steps like creating "tear line" reports, in which an agency produces a less classified, or unclassified version, along with the classified version, SHARE encourages reports that contain the maximum possible amount of sharable information.

In our suggested approach, the production of such alternate versions would be commonplace and automatic. And it would be a top priority. For example, an agency would create a "Top Secret/Code Word" report that reveals the source of the information; a "Secret" version that would not reveal the source, but might give explicit detail on the threat; and a "Sensitive But Unclassified" version that might only contain the necessary action the recipient agencies should take given their specific roles in the network (for example, to be on the lookout for certain individuals or indicators of specific terrorist activity).

INFORMATION SECURITY and AUDIT TECHNOLOGIES

In addition, SHARE would use existing technologies that can facilitate the sharing of sensitive information. For example, screening tools could be used to assist in the redaction process when moving information across security levels. Screening tools can automatically alert disseminators when potentially sensitive information is about to be transmitted, or when information may be about to be sent to parties that lack the requisite permission to receive it. Semi-automated systems could also suggest special-handling guidelines as well as who should be included on dissemination lists.

To address the need for information about reliability of a source without having to rely on classified descriptions, we recommend the use of "reputation meters" – similar to those used by e-bay to rate sellers –in formats for intelligence documents.

In addition, auditing technology, for example, could be deployed to track the flow of information to different players and to record how the information is used (whether, for example, it is printed, forwarded, or edited). This could help deter leaks. The auditing tools should use strong means of authentication that have forensic value (that is, they should be permissible in court to prove access). Information rights management technologies, when combined with digital certificates, can also help by allowing agencies to create self-enforcing rules about who can have access to particular documents, how they can be used, and how long the document can be viewed before access expires. Another possibility would be to make federal funding for information-sharing purposes contingent on the adherence to certain rules prohibiting unauthorized disclosure. Finally, information could be accompanied by clearer, more specific handling requirements and dissemination limitations. While none of these measures is perfect, a combination of such efforts might reduce the chance of unauthorized disclosure or uncoordinated action, and thereby foster a healthy environment for the sort of broad communication that we envision.

Conclusion

Recently, a number of agencies have been experimenting with creating systems to share information. For example the FBI is developing a new information-sharing policy and concept of operations that could instigate a "need-to-share" culture of distribution despite major barriers to adopt and implement the anticipated structure. And while this is a step in the right direction, an agency-by-agency approach will not work. What is needed is a

national framework that would enable change across the government as a whole and with state and local authorities as well to overcome the cultural barriers to information sharing.

Information sharing itself is not the goal; rather it is the means by which we can effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information. To accomplish this, we must shed our current Cold War "need to know" mentality and replace it with a culture based on the "need to share." Information security is a legitimate concern but can be appropriately addressed in ways that I have outlined above. What is needed now is the leadership – by both Congress and the President – to get the information flowing.

Thank you.