STATEMENT FOR THE RECORD

Ambassador Ted McNamara
Program Manager
Information Sharing Environment

House Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
April 26, 2007, 10:00 a.m. CHOB 310

I. Introduction

Chairwoman Harman, Ranking Member Reichert, and Members of the subcommittee: I am pleased to be here with my colleagues and want to thank you for your continued focus and priority to building an effective Information Sharing Environment (ISE).

As you and the Committee address classification of information issues, I would like to update you on a Presidential priority to standardize procedures for Sensitive But Unclassified (SBU) information. This is a priority because if we do not have a manageable SBU framework, we will not have an effective ISE.

Information vital to success in our protracted conflict with terrorism does not come marked "terrorism information"; it can and does come from many sources, including from unclassified information sources. Yet we lack a national unclassified control framework that enables the rapid and routine flow of information across Federal agencies and to and from our partners in the State, local, tribal and private sectors. This is especially important because some categories of unclassified information require controls as strong as those for national security information. There are sound reasons to protect those categories from public release, both to safeguard the civil liberties and legal rights of U.S. citizens, and to deny the information advantage to those who threaten the security or public order of the nation.

This lack of a single, rational, standardized, and simplified SBU framework is a major cause of improper handling. It heightens risk aversion and undermines confidence in the control mechanisms. This leads to both improper handling and unwillingness to share information. These problems are endemic within the Federal government, between Federal and non-Federal agencies and with the private sector. This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share information. They must share because they each have important responsibilities in countering terrorism. The problem exists at all levels -- Federal, State, local, tribal, and the private sector. All have cultures that are traditionally cautious to sharing their sensitive information, but this must be addressed if we are to properly and effectively share sensitive but unclassified information. Only when the Federal government provides credible assurance that it can protect sensitive data from unauthorized disclosure through standardized safeguards and dissemination controls will we instill confidence that sensitive information will be appropriately shared, handled, safeguarded, and protected, and thus make sharing part of the culture.

II. The Current SBU Environment

Let me note at the outset that I will focus here on "unclassified" information. Classified information is, by law and regulation, controlled separately in a single system that was established early in the Cold War years. The classification regime, currently governed by Executive Order 12958, as amended, applies to "national security information," which includes intelligence, defense, and foreign policy information. Other information, which legitimately needs to be controlled, is controlled by agency-specific regimes. Collectively, these regimes address information referred to as Sensitive But Unclassified (SBU) information. SBU information has grown haphazardly over the decades in response to real security requirements, but this information cannot be encompassed in the subject-specific classified control regime. The result is a collection of control mechanisms, in which most participants have confidence only when information is shared within an agency -- and sometimes not even then.

Let me give you some understanding of how complex SBU is: Among the twenty departments and agencies we have surveyed, there are at least 107 unique markings and more than 131 different labeling or handling processes and procedures for SBU information. Even when SBU information carries the same label marking (e.g. For Official Use Only), storage and dissemination are inconsistent across Federal agencies and departments. Because such markings are agency-specific, recipients of SBU information in a different agency must understand the processes and procedures of the originating Federal agency for handling the information, even if their agency uses the same marking. The result is an unmanageable collection of policies that leave both the producers and users of SBU information unable to know how a piece of information will be controlled as it moves through the Federal government and therefore reducing information sharing.

I would like to highlight just two examples to convey the confusion created by the current SBU processes:

The first example is a single marking that is applied to different types of information. Four agencies (DHS, DOT, USDA and EPA) use "SSI" to mean "Sensitive Security Information." However, EPA has also reported the use of "SSI" to mean "Source Selection Information" (i.e. acquisition data). These types of information are completely different and have vastly different safeguarding and dissemination requirements, but still carry the same SBU marking acronym. In the same way, HHS and DOE use "ECI" to designate "Export Controlled Information," while the EPA uses "ECI" to mean "Enforcement Confidential Information." "Export Controlled Information" and "Enforcement Confidential Information" are clearly not related, and in each case, very different safeguarding and dissemination controls are applied to the information.

The second example is of a single marking for the same information, but with no uniformity in control. Ten agencies use the marking "LES" or "Law Enforcement Sensitive." However, the term is not formally defined by most agencies nor are there any common rules to determine who can have access to "law enforcement information." Therefore, each agency decides by itself to whom it will disseminate such information. Thus, an individual can have access to the information in one agency but be denied access to the same information in another. Further confusing the situation, SBU markings do not usually indicate the originating entity. As a result, even if a recipient had access to all the different control policies for each agency, he or she could

probably not determine what rules apply because the recipient usually does not know which agency marked the document.

Protecting the sharing of information is a critical and interdependent function for the ISE. Simply stated, sensitive information will not be shared unless participants have confidence in the framework controlling the information. Standardizing SBU procedures is a difficult endeavor, made more complicated by the complex information management policies.

III. Unclassified Information Framework Imperative

Producers and holders of unclassified information which legitimately needs to be controlled must have a common framework for protecting the rights of all Americans. In the classified arena, we deal with information that will, mainly, be withheld from broad release. In the unclassified arena, we deal with information that is mainly shareable, except where statute and policy require restrictions. Agencies must often balance the need to share sensitive information, including terrorism-related information, with the need to protect it from widespread access.

A new approach is required. Existing practices and conventions have resulted in a body of policies that confuse both the producers and users of information, ultimately impeding the proper flow of information. Moreover, multiple practices and policies continue to be developed absent national standards. This lack of standards often results in information being shared inappropriately or not shared when it should be. In December 2005, the National Industrial Security Program Policy Advisory Committee described the consequences of continuing these practices without national standards in the following manner "…the rapid growth, proliferation and inclusion of SBU into classified contract requirements without set national standards have resulted in pseudo-security programs that do not produce any meaningful benefit to the nation as a whole." Clearly this situation is unacceptable.

IV. A Presidential Priority

The lack of government-wide standards for SBU information is well-known. More difficult has been charting a reasonable way ahead to create such standards. This is an enormously complex task that requires a careful balance between upholding the statutory responsibilities and authorities of individual departments and agencies, and facilitating the flow of information among them – all the while protecting privacy and civil rights. We were successful in creating such a regime for classified national security information by setting national standards and requiring that they be executed uniformly across the Federal government. In addition, we established a permanent governance structure for managing the classified information regime. A similar approach is necessary to establish an unclassified information regime, with standards governing controlled unclassified information.

As required by the Intelligence Reform and Terrorism Prevention Act of 2004, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*, which specified tasks, deadlines, and assignments necessary to further the ISE's development. Guideline 3, of his Memorandum, specifically instructed that to promote the sharing of , "…Sensitive But Unclassified (SBU) information, including homeland security information, law

enforcement information, and terrorism information[1], procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State; local, and tribal governments, law enforcement agencies, and private sector entities."

An interagency SBU Working Group, co-chaired by the Departments of Homeland Security (DHS) and Justice (DOJ), undertook an intensive study and developed several draft recommendations for a standardized approach to the management of SBU. Its work provided a solid foundation for completing the recommendations. It was determined, however, that additional work was necessary to fully meet the requirements of Guideline 3.

Recommendations for Presidential Guideline 3 are coming close to completion in a SBU Coordination Committee (SBU CC), chaired by the Program Manager, Information Sharing Environment (PM-ISE), with Homeland Security Council oversight. The SBU CC began work in October 2006 with the participation of the Departments of State, Defense, Transportation, Energy, Justice, and Homeland Security; the Federal Bureau of Investigation; the Office of the Director of National Intelligence; the National Security Council; and the Office of Management and Budget. The committee actively consults with representatives from other departments and agencies, the National Archives and Records Administration (NARA), the Information Security Oversight Office, the Controlled Access Program Coordination Office, the Information Sharing Council, the Global Justice Information Sharing Initiative, State, local, and tribal partners, and several private sector groups.

The efforts of the SBU CC have focused on developing an SBU control framework that is rational, standardized, and simplified, and as such, facilitates the creation of an ISE that supports the individual missions of departments and agencies and enhances our ability to share vital terrorism information among Federal, State, local, tribal, and private sector entities, and foreign partners.

- RATIONALIZATION means establishing a framework based on a set of principles and procedures that are easily understood by all users. This should help build confidence among users and the American public that information is being shared and protected in a way that properly controls information that should be controlled, and protects the privacy and other legal rights of Americans.

- STANDARDIZATION means structuring a framework in which all participants are governed by the same definitions and procedures and that these are uniformly applied by all users. The objective is to end uncertainty and confusion about how others using the framework will handle and disseminate SBU information.

[1] Pursuant to the ISE Implementation Plan, and consistent with Presidential Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

Standardization helps achieve the ISE mandated by Congress: "a trusted partnership between all levels of government."

- SIMPLIFICATION means operating a framework that has adequate, but carefully limited, numbers and types of markings, safeguards, and dissemination of SBU information. Such a simplified framework should facilitate Federal, State, and local government sharing across jurisdictions; facilitate training users; and reduce mistakes and confusion.

V. The Controlled Unclassified Information (CUI) Framework

I must reiterate that interagency discussions of a proposed detailed framework are still underway. Furthermore, no recommendation will become final unless and until it is approved by the President. Of course, the ability to implement any reform will depend upon the availability of appropriations. With respect to the present proposal, however there is general agreement that the SBU framework should include the following six main elements:

1. CUI DESIGNATION: To ensure a clean break with past practices, the Framework would change the descriptor for this information to "Controlled Unclassified Information" (CUI) – thus eliminating the old term "SBU." Participants would use only approved, published markings and controls, and these would be mandatory for all CUI information. All other markings and controls would be phased out.

2. CUI MARKINGS: The CUI Framework also contains mandatory policies and standards for marking, safeguarding and dissemination of all CUI originated by the Federal government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal. This Framework includes a very limited marking schema that addresses both safeguarding and dissemination. It also provides reasonable safeguarding measures for all CUI, with the purpose of reducing the risk of unauthorized or inadvertent disclosure and dissemination levels that with the purpose of facilitating the sharing of CUI for the execution of a lawful Federal mission or purpose.

3. CUI EXECUTIVE AGENT: A central management and oversight authority in the form of an Executive Agent would govern the new CUI Framework and oversee its implementation.

4. CUI COUNCIL: Federal departments and agencies would advise the Executive Agent through a CUI Council composed of senior agency officials. The Council will also create mechanisms to solicit State, local, tribal, and private-sector partner input.

5. ROLE OF DEPARTMENTS AND AGENCIES: The head of each participating Federal department and agency will be responsible for the implementation of a functional CUI Framework within the agency.

6. CUI TRANSITION STRATEGY a Transition Strategy for a phased transition from the current SBU environment to the new CUI Framework is needed. During the transition, special attention would be paid to initial governance, performance measurements, training, and outreach components.

On a final note, our work has recognized that the substantive information that will be marked and disseminated in accordance with the proposed Framework is also subject to a variety of other legal requirements and statutes. Among some of the most important statutes and legal authorities that apply to this information are the Privacy Act of 1974, the Freedom of Information Act, the Federal Information Security Management Act (FISMA) and various Executive Orders, including Executive Order 12333, which governs the Intelligence Community and its use of United States Persons information. I would like to stress that this proposed Framework for handling SBU has thoroughly considered these legal authorities and does not alter the requirements and obligations imposed by these authorities. We will continue to work with the ISE Privacy Guidelines Committee to ensure that the appropriate privacy issues fully meet any legal requirements to protect the civil liberties and privacy of Americans.

VI. Conclusion

"*For information sharing to succeed, there must be trust—the trust of government providers and users of information, or policymakers, and most importantly, of the public. Each of these must trust that information is being shared appropriately, consistent with law, and in a manner protective of privacy civil liberties. Building trust requires strong leadership, clear laws and guidelines, and advanced technologies to ensure that information sharing serves important purposes and operates consistently with American values.*"[2]

The lack of a single, rationalized, standardized, and simplified SBU framework does contribute to improper handling or over-classification. To instill confidence and trust that sensitive information can be appropriately shared, handled, safeguarded, and protected, we must adopt a standardized CUI Framework. This is especially critical to our counterterrorism partners outside the intelligence community. Appropriately protecting law enforcement and homeland security related sources and methods are just as valuable to our national security as protecting our intelligence sources and methods.

The global nature of the threats our Nation faces today requires that: (1) our Nation's entire network of defenders be able to share information more rapidly and confidently so that those who must act have the information they need, and (2) the government can protect sensitive information and the information privacy rights and other legal rights of Americans. The lack of a government-wide control framework for SBU information severely impedes these dual imperatives. The CUI Framework is essential for the creation of an ISE which has been mandated by the President and the Congress. Only then can we meet the dual objectives of enabling our Nation's defenders to share information effectively, while also protecting the information that must be protected. A commitment to achieving standardization is essential–a vital need in the post-9/11 world.

[2] *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, Third Report of the Markle Foundation Task Force, July 2006