Testimony by Scott Armstrong
Director, Information Trust
to 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 Information"

June 28, 2007

10:00 a.m., 311 Cannon House Office Building
House of Representatives
Committee on Homeland Security
Washington, D.C. 20515

Chairwoman Harman, Ranking Member Reichert, and members of the Committee, thank you for this opportunity to address the issues of classification and pseudo-classification at the Department of Homeland Security.

My views today are my own, but I should note that I have been working closely with the Aspen Institute to sustain a six-year Dialogue between senior journalists, editors and publishers and high level US government officials from various national security and intelligence agencies, including senior members of congress and their staffs. The Dialogue on Journalism and National Security has attempted to address recurring concerns about the handling of sensitive national security information by government officials and representatives of the news media. The discussions have included the Attorney General, the Director of the Central Intelligence Agency and ranking officials from the National Security Council, the Department of Defense, the National Security Agency, the FBI as well as the CIA and the Department of Justice.

The Dialogue grew out of mutual concerns that legislation passed by both Houses of Congress in 2000 was, in effect, America's first Official Secrets Act. Although vetoed by President Clinton, the bill was reintroduced in 2001. In the wake of 9/11, high ranking officials of the national security community and the leadership of national press organizations recognized that the disclosure of sensitive national security information was a reason for concern. We found considerable agreement that legislation which inhibited virtually all exchanges of sensitive information -- even responsible exchanges designed to increase public appreciation of national security issues -- was not likely to make America more secure.

The goal, we seemed to agree, has been to have a well-informed citizenry that is assured of its safety without sacrificing its liberty. The lessons of 9/11 focused on

sharing more information within government agencies, laterally across federal agency barriers and among federal, state, local governments and with critical private industries, community first responders and the public at large.

The Homeland Security Information Sharing Act, first passed by the House in 2002 and incorporated into the Homeland Security Act of 2004,[1] mandated the creation of a unique category of information known as "sensitive homeland security information." This category of SHSI information -- as we have transliterated the acronym – was designed to permit the sharing of certain critical information with state and local authorities without having to classify it and require its recipients to hold clearances thus creating new barriers to communication. At the same time, SHSI designates information deemed necessary to withhold briefly from the general public while appropriate measures are taken to protect our communities.

The challenge for the Department of Homeland Security is not so much how to WITHHOLD secrets from the public and its local governmental representatives. The challenge is how to SHARE information so as to promote our security. For once government's first mission is not to silence "leaks," but to effectively share official information outside its usual restraints.

The discipline of controlling information needs to give way to the creative task of selecting previously withheld information and pushing it rapidly and articulately out to the extraordinarily varied organizations that protect us: local law enforcement; first responders; medical and emergency response teams; community

[1] PL.107-296

leaders; utility industry managers with nuclear facilities or farms of chemical and energy storage tanks; mass transportation operators, and so forth.

Homeland security requires the vigilance of the many rather than the control of the few. Awareness, prevention, protection, response and recovery are not hierarchical tasks dictated from the top. Secrecy must yield to communication. This is no trivial task. The mission of information sharing is difficult enough within the cumbersome and slumbering giant newly merged from dozens of agencies and populated more than 180,000 employees. But that job is only the beginning since DHS is the focal point for leveraging some 87,000 different governmental jurisdictions at the federal, state, and local level which have homeland security responsibilities involving tens of millions of Americans whose responsibilities cannot be choreographed from afar, but must be inspired by shared information.

In the National Intelligence Reform Act of 2004, the Congress took another major step to address this phenomenon. It authorized broad centralized power for the new Director of National Intelligence and urged the new DNI to create a tear-line report system by which intelligence gathered by an agency is prepared so that the information relating to intelligence sources and methods is easily severable within multiple layered products to allow wide sharing while protecting truly sensitive sources and methods from unauthorized disclosure.

The benefit to the protection of our communities lies on the other side of that "tear-line" system. By concentrating on the classification guidelines for protecting well-defined sources and methods and making refined decisions to protect that which truly requires protection, more of the remaining information should be available for sharing within the intelligence community as well as within the diversified and

distributed elements of the colossus of those charged with Homeland Security responsibilities. The public benefits from these designations within internally published intelligence requiring protection because it makes majority of fact and analysis available for expedited release -- not just to homeland security organizations -- but also to the media and the public.

Your attention today follows a series of extraordinary efforts by this administration to control information with such severity and vengeance that it has blinded its constitutional partners here and in the judiciary. Most startling, this administration has used these information controls to institute policy and decision making layers which have doomed even senior departmental officials to work in the sort of isolated stovepipes described in the repetitious texts of 9/11 failures.

This is no longer a question of issues of over-classification but one of wholesale compartmentalized control and institutionalized intimidation through the use of draconian Non-Disclosure Agreements. It appears designed more to inhibit and constipate internal communications in the federal government than to protect the national security.

Not surprisingly, the Department of Homeland Security wasted no time in replicating the move to Non-Disclosure Agreements (NDA's). But it combined it with an effort to side-step the congressional mandate to foster information sharing. Rather than educate the rest of the government on how to effectively communicate information, DHS dispersed new information control authority across the full spectrum of executive agencies. The uncoordinated proliferation of Sensitive But Unclassified designations – of the sort you address today -- already includes some remarkable missteps.

In one instance, the Department of Homeland Security drafted a draconian Non-Disclosure Agreement (NDA) designed to impose restrictions on tens of thousand federal employees and hundreds of thousands of state and local first responders. This NDA[2] for unclassified information more severe than the NDA's covering Sensitive Compartmented Information and even more sensitive information under the government's control.

This NDA required officials, employees, consultants and subcontractors to protect such "sensitive but unclassified information," which is defined as "an over-arching term that covers any information … which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy [of] individuals … but which has **not** been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and **any other identifier used by other Government agencies** to categorize information as sensitive but unclassified.**"**

This overbroad -- but legally binding requirement -- was implemented as a condition of access to certain unclassified information. Such an NDA represented a vast increase in government secrecy. It left control in the hands of an undefined and virtually unlimited number of supervisors. Those who signed the agreement

[2] DHS Form 11000-6 (08-04) See Attached Exhibit A

were bound perpetually until it was explicitly removed. The NDA had no statutory authority and thus no defined criteria, rules, limitations or effective oversight. Although it did not provide an explicit rationale for withholding "Sensitive But Unclassified" information under the Freedom of Information Act, it surely provided an incentive to err in favor of using other exemptions to deny release.[3]

Although this NDA was withdrawn by DHS in January 2005, it was used last year at the Department to silence private Wackenhut guards who were speaking to the press about security breakdowns at the Department's Nebraska Avenue headquarters. Other instances of SBU constraints by government agencies, contractors and utilities appear to be used most often to discourage and prevent the public from participating in its government. Provisions similar to the DHS NDA have since appeared in other employee and contractor agreements both within DHS and within other departments.[4]

I repeat the details of DHS's failed practices to underline the suggestion that DHS is dramatically out of synch with its mandate to increase our security at home by aggressively -- and yet carefully -- sharing information in order to frustrate terrorists through prepared and coordinated responses of the most sophisticated intelligence capabilities on one hand, and our most formidable first line of defense -- local law enforcement and first responders, on the other hand.

The Necessary Response

Adopt into legislation features which directly address your intentions.

[3] See also DHS directive (MD 11042) on "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," dated May 11, 2004.

[4] See CRS Report RL33303, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, February 15, 2006 Genevieve J. Knezo, Specialist in Science and Technology Policy, Resources, Science, and Industry Division.

1. **DHS is the right place to begin**. The current classification system within government is out of control and likely uncontrollable. Someone needs to start over with a new test-bed. DHS, with its critically mission of communicating effectively across the federal government and with all other layers of state and local institutionsm has the greatest incentive for change.
2. **Give DHS near-term objectives** and extra resources to achieve concrete results. Hold the Secretary of Homeland Security accountable for the mandates contained in the law which dispensed such sweeping power.
3. The **DNI has the authority** to mandate DHS as a test-bed and to direct other departments and agencies to cooperate in changing the range of intelligence and information control systems. Hold the DNI accountable by regularly measuring achievements within organizations under his control.
4. Provide **built-in monitoring** by independent and experienced observers such as the **Information Security Oversight Office and the Public Interest Declassification Board** and provide the monitors with the resources to do their job.
5. The **tear-line system** designated by Congress four years ago is the right standard. It needs major attention to standardize guidance materials which can be applied with precision. All intelligence publication and sharing should be premised on carefully and formally defining sources and methods which require protection by isolating the smallest number of critical details. Information which requires less protection will receives greater circulation and earlier decontrol.
6. Provide **training and performance evaluation** incentives throughout all levels of DHS, in order to assure that the information which needs tight sources and methods control – and only that information – receives the ultimate protection.

7. Create **an electronic metadata tagging system** which requires that rigorous classification decision making will follow established guidance. Use it to assure that all levels understand they must conform with established practice and their effectiveness can and will be calibrated. Such a tagging system not only improves accountability, but also allows corrections and the protection of information improperly handled.
8. Demand and reward **less information control** in order to **maximize communication**.
    - Changing goals require reinforcement that **professionalizes** every level and every aspect of the information control process.
    - Translate Information Control Guides (Classification Guides) into **action directives about what and how to communicate** rather than simply what and when information might be declassified or decontrolled.
    - Provide opportunities for training and conceptual exercise which insist on communication up and down the line as well as lateral reviews and find mechanisms to make sure that the **communication runs to, as well as from, all intended recipients**.
9. Hold **government officials and employees accountable** for their decisions.
    - When mistakes come to light, **reeducate and retrain**.
    - Rethink the scope and purpose of both past practices and contemporary innovations by insisting **managers manage** the process with a willingness to keep changing procedures until they truly work.
    - **Remove authority** from those who abuse it.
    - Hold **supervisors responsible** by requiring them to assume **additional monitoring and training responsibilities if those reporting to them fail** to perform well-defined and specifically designated responsibilities. Similarly reward them when their aides perform their communication roles well.

- **End the incentive to classify** simply because over classifying has no consequences to individuals but information released can be career ending.
- Institute pro-active audits and correlated retraining.
- Allow government employees and motivated citizens – such as users of the FOIA – to bring mistakes to light. Follow-up in a transparent manner to demonstrate that improved communication and improved information controls are not necessarily on separate planes but are integrated concerns of all stakeholders in a democracy.

10. Encourage the Office of the DNI and full range of Agencies under DNI authority -- including but not limited to DHS -- to take careful cognizance of the **well established tradition of background briefings in which national security officials and the media communicate informally** in a manner meant to inform the public (including the Congress and others in the Executive) and provide a degree of confidence that secrecy is not being used to erode or impede civil liberties and free expression.
    - Include training for national security officials on responsible interaction with the news media **by including the news media in the training**
    - Offer the **media opportunities to learn about the laws, regulations and practices which involve secrecy** and other national security protocols.

We would all do well to recall that our freedom has been protected and our homes have been secure because -- as a people – we have understood how to best to share information and how best to respond together to mutual threats.

Exhibit A

Department of Homeland Security Form

DHS Form 11000-6 (08-04)

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT