Statement
Of
Patrice McDermott
Director
OpenTheGovernment.org

Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment
Committee on Homeland Security
On
H.R. 6193, The "Improving Public Access to Documents Act,"
Wednesday, June 11, 2008
219 Cannon HOB
10:00 A.M.

Thank you, Chairwoman Harman, Mr. Reichert, and Members of the Subcommittee, for the opportunity to speak today on the proposed legislation that would require the implementation of the Controlled Unclassified Information framework within the Department of Homeland Security in a manner that will ensure, promote and improve public access to documents within, and those shared with and by, the Department.

My name is Patrice McDermott. I am the Director of OpenTheGovernment.org, a coalition of consumer and good government groups, library associations, journalists, environmentalists, labor organizations and others united to make the federal government a more open place in order to make us safer, strengthen public trust in government, and support our democratic principles.

Background

"Fundamental to our way of life is the belief that when information which properly belongs to the public is systematically withheld by those in power, the people soon become ignorant of their own rights, distrustful of those who manage them, and – eventually – incapable of determining their own destinies."

The author of that statement was Richard M. Nixon in March 1972, in his "Statement on Establishing a New System of Classification and Declassification of Government Documents Relating to National Security." President Nixon had it right.

Three years ago, in our 2005 Secrecy Report Card[1], we identified 50 types of restrictions on unclassified information, implemented through laws, regulations or mere assertions by government officials that information should not be released to the public. These designations fall entirely outside the national security classification system, which is governed by executive order, and they are subject to none of its constraints or timelines.

[1] http://www.openthegovernment.org/otg/SRC2007.pdf

GAO, in a 2006 report[2], identified 56 designations. While different agencies may use the same marking to denote information that is to be handled as SBU, a chosen category of information is often defined differently from agency to agency, and agencies may impose different handling requirements. Some of these marking and handling procedures are not only inconsistent, but are contradictory. Some protections are necessary for unclassified information, such as personal privacy information or trade secrets – which are protected by statutes and exemptions to the FOIA that openly cover them.

GAO found that more than half the agencies reported challenges in sharing such information. Thirteen agencies designate information For Official Use Only, which does not have prescribed criteria. Sometimes agencies used different labels and handling requirements for similar information and, conversely, similar labels and requirements for very different kinds of information. The numerous designations can be confusing for recipients of this information, such as state and local law enforcement agencies, which must understand and protect the information according to each agency's own rules. It is clear that the unconstrained proliferation of these tags has not been a boon to sharing – or to the safety and security of the American public.

Most of the agencies GAO reviewed have no policies for determining who and how many employees should have authority to make sensitive but unclassified designations, providing them training on how to make these designations, or performing periodic reviews to determine how well their practices are working. They seem to be applied with little thought and, according to a 2005 New York Times story,[3] employees could visit the agency's Web site and easily print out a bright-yellow "sensitive security information" cover sheet.

Also, clearly not all of the categories listed by the agencies in GAO's report should be included as "sensitive but unclassified" designations. Exemptions created by the Freedom of Information Act (other than by what are called (b)(3) statutes) and the Privacy Act) do not logically constitute what we understand as SBU-like designations (i.e., as generally having little grounding in statute and as limiting access to otherwise public information). Nevertheless, the agencies apparently think of them in this way. It is important to note that the new Controlled Unclassified Information (CUI) Framework recently announced will apply only to agency-generated markings. It will not apply to statutorily-created restrictions, including (b) (3) exemptions to the Freedom of Information Act – which are also proliferating.

As you know, the White House issued a Memorandum to all heads of Executive departments and agencies a month ago. The intent of the Memorandum is to contain and constrain the proliferation of unclassified control markings – within the Information Sharing Environment. The goal is to standardize practices to facilitate and enhance the sharing of what is now called Controlled Unclassified Information, but only with and among those who are already sending and receiving it.

---

[2] GAO: March 2006: Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information: GAO-06-385 http://www.gao.gov/new.items/d06385.pdf

[3] http://www.nytimes.com/2005/07/03/politics/03secrecy.html

Default must be openness

We are very pleased that you have designated your legislation as the "Improving Public Access to Documents Act of 2008. As you note in the Findings section, the proliferation of SBU control markings needlessly limits public access to information, and increases the costs of information security, which are already extraordinarily high. Indeed, assessing the costs associated with creating and safeguarding CUI are something that you may want to consider adding to the important auditing mechanism this bill creates.

The White House Memorandum makes only a minimal nod toward public access and no acknowledgement of the benefits of openness to our society and to our safety. This bill takes important steps toward ensuring that those benefits are considered in decisions about whether and how to put controls on access and disclosure of information that might be considered as CUI.

The default bureaucratic position is to not take risks. Unfortunately, the message that has been given to officials in our government is that openness is risky. This is not only a dangerous mindset in an open society, but, as the findings to the legislation under discussion today note, it stands in the way of a safer and more secure homeland. We are all agreed that there is information that does need to be protected for some period of time. The tension, though, is not between openness and security; it is between information control for bureaucratic turf, power, and more than occasionally political reasons and the reality that empowering the public makes us safer. Secrecy does not make for a more secure society; it makes for a more vulnerable society and less accountable governments.

To counter the impulse toward non-disclosure, the bill has three provisions that we think are very important. We urge you to protect these provisions throughout the legislative process to ensure their inclusion in any final legislation that may be signed into law.

The first set of these establishes that CUI markings are not a determinant of public disclosure pursuant to the Freedom of Information Act. As I noted earlier, the 2006 GAO clearly indicated that the agencies think of several of the FOI exemptions as creating control categories. The effect on access to information through FOIA has been pernicious, from what we have heard from the requestor community. To ensure that this provision is properly implemented, the legislation contains two critically important requirements. The Department is required to

- maintain a publicly available list of documents designated and marked, in whole or in part, as controlled unclassified information, indicating which have been withheld in response to a request made pursuant to section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act'); and

- create a process through which the public may seek the removal of such a designation and marking.

The list of documents is essential not only for ensuring that CUI markings do not preclude disclosure under the FOIA, but also as a critical tool for oversight and for

maintaining a check on agencies' demonstrated impulse to over-control and over-designate information.

The creation of a process empowering employees to challenge the use of CUI marking and to be rewarded for successful challenges resulting in the removal of the markings is an additional safeguard of public accountability. It is critical, however, that the legislation also ensure that employees do not face reprisals for protecting openness. The legislation should clarify that disclosures of any violation of applicable procedures, including those made in the course of an employee's routine job duties or in the context of an Inspector General audit, are protected under the Whistleblower Protection Act (WPA). Over the years, employees routinely have lost whistleblower retaliation cases because of activist interpretations of the whistleblower law that removed protection for employees in similar contexts. Employees need to know they will be protected from reprisal for helping to enforce the provisions of this Act.

The second key set of provisions, critical to ensuring maximal openness, concerns controlling the controllers. The legislation takes two strong steps in this direction. The first is a requirement that the Department's CUI framework ensure that the number of Department employees and contractors with original and derivative CUI designation authority is appropriately limited – as determined through consultation with stakeholders designated in the bill.

The second provision requires the tracking, by particular employee, of the marking of documents, when and how they are shared, and the misuse of CUI marking. This capability is key both to the IG auditing mechanism established by the bill and to evaluation and promotion decisions about individual employees.

These are each important improvements on the White House Memorandum and we will urge NARA to adopt them for government-wide implementation.

Process must be as open as possible

The third key provision that we urge you to protect throughout the legislative process is the inclusion of organizations with expertise in civil rights, civil liberties, and government oversight in the list of those with whom the Department must consult in the development of policies, procedures and programs to implement the CUI framework within the Department. Meaningful engagement with such organizations is critical both to ensure the proper implementation of the important provisions of the legislation noted above, and to foster public trust in the application of the markings and the information that is shared within the information sharing environment.

The White House Memorandum enshrines the practice to date, which is to include only State, local, tribal, and private sector entities in the process. The argument made to those of us on the outside is that only these entities have responsibility for marking and handling CUI. This Committee understands that the benefits of openness and the risks to

privacy, civil rights, and civil liberties can easily be lost or forgotten in such inner-circle discussions. Members of the public are also stakeholders in this process.

Information Sharing must include the public

We have experienced a trend in our country away from trust in the public to a "need-to-know" mind set. A few, primarily federal, departments and entities have either, in a few cases, been designated or have arrogated to themselves the power to say who has a need-to-know and only governments and a few private sector entities have been deemed worthy. The public and the press have been almost entirely excluded. At one point, the Department of Homeland Security even attempted to make Congressional staff sign non-disclosure agreements in order to prove they could be trusted into the inner circle of those legitimate few.

Again, there is absolutely some finite amount of information that, for a certain amount of time, needs to be shared only in a limited fashion. The problem for the public is that we have "translucence, not transparency, i.e., transparency within the network, but opacity to those outside."[4] The "need-to-share"" cannot be limited to agencies within governments and defense and homeland security contractors; it also must include, to the greatest extent possible, sharing relevant information with the public. The White House Memorandum and this legislation both recognize this by requiring "portion marking," so that information in a document that is eligible for disclosure can be made public.

We look forward to opportunities to work with you on this bill and to ensure that this legislation begins the process of ensuring that public access to documents, including CUI, within the Department of Homeland Security is truly improved.

Thank you, again, for this opportunity to discuss this critical issue and your bill. I will be pleased to answer any questions.

[4] Elizabeth Rindskopf Parker, "Translucence Not Transparency: Reviewing Alasdair Roberts, Blacked Out: Government Secrecy In The Information Age." I/S: A Journal Of Law And Policy For The Information Society, Vol. 2, Issue 1 (2006). http://www.is-journal.org/V02I01/2ISJLP141.pdf