H.R. 6193, THE "IMPROVING PUBLIC ACCESS TO DOCUMENTS ACT OF 2008"

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 11, 2008

Serial No. 110–121

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

44–047 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey
PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*
DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

CONTENTS

H.R. 6193, THE "IMPROVING PUBLIC ACCESS TO DOCUMENTS ACT OF 2008"

Wednesday, June 11, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:06 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chair of the subcommittee] presiding.

Present: Representatives Harman, Langevin, Carney, Reichert, and Dent.

Ms. HARMAN. The subcommittee will come to order.

We expect other members to arrive shortly. But the Ranking Member and I are here, and we are ready to begin with our all-women panel.

I have to tell you before I do anything else that the Ranking Member just told me that when he was sheriff in Washington State, his entire command staff was female, and many of his other key jobs were held by females, and that, of course, is why he was successful.

Ms. MCDERMOTT. There you go.

Ms. HARMAN. The subcommittee is meeting today to receive testimony on H.R. 6193, the "Improving Public Access to Documents Act of 2008."

From the start of the 110th Congress, this subcommittee has focused on two huge obstacles to accurate, actionable and timely information-sharing: first, our Nation's broken classification system; and, second, the explosion in the number and use of "sensitive but unclassified" control markings. Later today, the subcommittee will take legislative action to address these twin problems with a mark-up of H.R. 4806, the "Reducing Overclassification Act of 2007," and a new bill that is the subject of today's hearing.

Last Thursday, Dave Reichert and I were joined by six other members of the Homeland Security Committee in introducing H.R. 6193, the "Improving Public Access to Documents Act of 2008," the so-called IPAD Act. The IPAD Act will give life to the newly released Controlled Unclassified Information Framework—that is a mouthful—prepared by the program manager of the information-sharing environment, Ambassador Ted McNamara, who is well-known to this subcommittee and who testified before us on this subject last spring.

Wherever you are, Ambassador McNamara, we commend you for crafting a framework that appears to be a workable replacement for the out-of-control SBU practices, policies and procedures that have plagued the Federal Government. Indeed, some 28 distinct policies for the protection of "sensitive but unclassified" information presently exist. Security experts believe that there are more than 100 individual agency control markings that have stymied both the sharing of unclassified information within the Intelligence Community and disclosures of that information to the public.

Unlike classified records, moreover, there has been no monitoring of the use or impact of SBU control markings. Ambassador McNamara's CUI framework promises to bring order to the chaos. Ranking Member Reichert and I and our Members want to help. The legislation we have put together requires the Department of Homeland Security to adopt the new CUI framework implementation plan with rigorous policy development, training and auditing requirements. Accountability is what will make this new approach succeed, and the IPAD Act is aimed at getting it right.

After working together on the bill for months and now with significant input from the privacy, civil liberties and government oversight communities, we believe the legislation will make DHS the gold standard when it comes to getting the CUI framework up and running and working.

The potential dividends for more and better homeland security are enormous. Implementing the new framework at DHS will not only improve information-sharing with the Department's State, local and tribal partners but also will help decrease the exorbitant information security costs that the current SBU regime imposes and undo misguided SBU control marking practices that needlessly limit public access to information.

Bottom line, doing this will improve public access to information. The public has a right to know about material in many of these documents. These markings cannot be an excuse to cover material up, to protect somebody's either political interests or mistakes.

That is why I am glad to be joined by our three female witnesses today. Each will be sharing her views on how the IPAD Act will promote not only more robust information sharing within Government and with the public, but also more transparency regarding how our Nation is working to secure itself from terrorist attacks.

That transparency will foster greater public confidence by requiring DHS to keep faith with the Constitution and the rule of law as it does its work. That may sound a little trite, but keeping faith with the Constitution and the rule of law may have been lost in some of these overclassification and pseudo-classification exercises in recent years.

I want to thank our Ranking Member and our other Members for supporting the critical legislation, and look forward to the witnesses' testimony this morning.

I now yield to Sheriff Reichert, employee of many senior females in his past occupation, for his opening remarks.

Mr. REICHERT. Thank you, Madam Chair. I do have to say, we, in the last year-and-a-half, have developed a great friendship and a great working relationship, and it is built on trust. I think, as you hear my opening statement, I will mention that, because I

think the information-sharing system is a system that must be built on trust also. I think everyone would agree to that. You know, there are a lot of directions that we come at this, but it has been a joy and pleasure to work with you, Madam Chair, on this issue.

Both of our hearts are at a place where we really believe that this legislation and some of the others that we will consider today is very, very important to the protection of our country and our community and also the protection of our civil liberties and the rights that we enjoy under the protection of the Constitution, guaranteed to us by the Constitution.

My job as the sheriff was to, of course, make sure that those laws were enforced and that we did protect people and ensure that their rights were protected too. So here I am in a little different role but certainly understanding where we are going with this. I have worked with this at a local level with a lot of Federal agencies.

So I want to thank you all for being here today to talk about H.R. 6193, the "Improving Public Access to Documents Act." I applaud the intent of this legislation to make sure that information that needs to be protected remains protected and information that should be disclosed is available to the public.

It is essential that the brand-new controlled unclassified information, CUI, framework is successful. Designating a document CUI to protect sensitive information will directly help fix the overclassification issues and problems that are rampant in our Federal Government.

Currently, agencies often overclassify information as "secret" because they do not trust the protections for "official use only" and "sensitive but unclassified." Because misunderstanding of these markings often leads to public disclosure of sensitive information, agencies would rather stamp "secret" on the document because they know it will be protected.

Consolidating all of these legacy markings under the new CUI framework will help our Federal Government protect information in a way that allows for quick sharing with State and local law enforcement and other public and private stakeholders that may not have clearances.

But as I have heard and experienced over and over again, information sharing, as I said earlier, is really about trust. We need to ensure that when we implement any final CUI framework it will not only apply to the Department of Homeland Security but all Government agencies. We cannot have the FBI or the CIA and other Federal law enforcement and intelligence agencies distrusting the process and keeping their information from DHS. That is a concern that I think both the Chair and I share.

As I said, I have witnessed some of this in my days as the sheriff. Information-sharing breaks down in the same—you know, as you work with other agencies, if you have a different set of standards, I have discovered that the FBI, DEA, ATF—of course, when they supplied information to the sheriff's office back in my days, they were then subject to the public disclosure laws of the State of Washington, and therefore the information they shared with us was open to request. So there was a reluctance then to share that information. However, we were successful in some instances in prying that information loose. It was not easy, however.

So I look forward to working with all of you. I sure appreciate you being here this morning, and I look forward to your testimony.

Again, it has just been a pleasure to work with the Chair on these important bills. I yield back the balance of my time.

Ms. HARMAN. I thank the Ranking Member for his comments. Moments of bipartisanship are all too rare around here. As I was telling our witnesses just before the hearing, I expect that we will not only have bipartisan support for this bill and the others I mentioned but unanimous support, as we mark them up later today. Everyone should focus on that short moment because, come tomorrow, other things may overtake this. But this is what Congress should be about, in my view, and that is working together to solve hard problems. I believe we have a very good solution before us.

Other Members have not arrived, so I don't need to announce that their statements will be inserted for the record.

I welcome our witnesses this morning.

Our first witness, Meredith Fuchs, is the general counsel of the National Security Archive, an independent nongovernmental research institute and library at the George Washington University that collects and publishes declassified documents obtained through the Freedom of Information Act.

I was talking to Ms. Fuchs about one of the founders of the National Archive, Scott Armstrong, who has been a witness before us and who is a valued friend and has been consulted by us often, as we develop not just this legislation but other things. I just want to send my enormous wishes to Mr. Armstrong.

Ms. Fuchs previously was a partner with the law firm of Wiley, Rein and Fielding here in Washington, where she developed a significant e-commerce and privacy practice. She is a frequent lecturer and author on both data privacy and e-commerce liability issues. Formerly a Supreme Court assistance project fellow with the Public Citizen Litigation Group, and also a law clerk with the U.S. Court of Appeals for the District of Columbia and the U.S. District Court for the District of Columbia.

She is a graduate of New York University School of Law.

Our second witness, Patrice McDermott, is the director of OpenTheGovernment.org, an organization that seeks to advance the public's right to know and to reduce secrecy in government.

She previously served as the deputy director of the Office of Government Relations at the American Library Association's Washington office, where she had lead responsibility for government information and privacy policy and e-government policy issues.

Ms. McDermott has also served as the assistant director for the Office of Intellectual Freedom of the American Library Association, taught information politics at Clark Atlanta University, and worked at the National Archives and Records Administration.

She has her doctorate in political science from the University of Arizona and is the author of "Who Needs to Know? The State of Public Access to Federal Government Information."

Our third witness, Caroline Fredrickson, is the director of the Washington legislative office of the ACLU. She is the organization's top lobbyist and supervises a nearly 60-person team in promoting ACLU priorities in Congress.

Ms. Fredrickson has years of experience as a senior staffer on Capitol Hill, having previously served as chief of staff for Senator Maria Cantwell and as deputy chief of staff to Senate Minority Leader Tom Daschle.

In 1998 and 1999, she was special assistant to the President for legislative affairs, a position that required her to work closely with both parties in the Senate to forge bipartisan agreements on the White House's legislative priorities.

Ms. Fredrickson is a Colombia University Law School graduate, where she was a Harlan Fiske scholar.

Without objection, the witnesses' full statements will be inserted in the record. I understand we have some letters of support for the bill from both the organizations you represent and other organizations. Without objection, they, too, will be inserted in the record.

[The information follows:]

WASHINGTON
LEGISLATIVE OFFICE

June 5, 2008

The Honorable Bennie Thompson
U.S. House of Representatives Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515-6480

The Honorable Jane Harman
U.S. House of Representatives Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment.
H2-176 Ford House Office Building
Washington, DC 20515-6480

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6th FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
www.aclu.org

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18th FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

RE: The Reducing Over-Classification Act of 2008

Dear Chairman Thompson and Chairwoman Harman,

On behalf of the American Civil Liberty Union, its hundreds of thousands of members and fifty-three affiliates, we write in support of the "Reducing Over-Classification Act of 2008."

As the findings in the bill indicate, over-classification interferes with the timely sharing of accurate and actionable information, unnecessarily increases government costs, and needlessly limits public access to information. We commend Representative Jane Harman for taking this important step toward creating a more accountable government by compelling the Department of Homeland Security to develop policies and programs to prevent the over-classification of homeland security information. Requiring the DHS Secretary to coordinate and consult with the Archivist of the National Archives and Records Administration, State, local and tribal governments, civil liberties groups, government oversight organizations, and the private sector will ensure that all stakeholders have a say in the development of these DHS policies and procedures.

There are important provisions in the bill that create mechanisms to make the classification process more accountable. They include a rewards program for successful challenges to classification decisions, an Inspector General audit requirement and a requirement to develop an electronic tracking system for classification decisions by particular employees, with penalties for failure to follow the over-classification reduction policies. The requirement to produce simultaneous unclassified versions of finished intelligence products will insure important information is available to State, local and tribal governments, and to the public at large.

We commend you for drafting a bill that encourages transparency in government and requires implementation of policies to maximize sharing of documents with the public.

Again, we thank you and your staffs for your open consultation with us with respect to your draft legislation. We look forward to working with you on this bill as it moves through the legislative process.

Sincerely,

Michael W. Macleod-Ball
Chief Legislative and Policy Counsel

Michael German
Policy Counsel

Timothy Sparapani
Senior Legislative Counsel

WASHINGTON
LEGISLATIVE OFFICE

June 5, 2008

The Honorable Bennie Thompson
U.S. House of Representatives Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515-6480

The Honorable Jane Harman
U.S. House of Representatives Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment.
H2-176 Ford House Office Building
Washington, DC 20515-6480

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6th FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.544.0738
www.aclu.org

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18th FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

RE: The "Improving Public Access to Documents Act of 2008"

Dear Chairman Thompson and Chairwoman Harman,

On behalf of the American Civil Liberty Union, its hundreds of thousands of members and fifty-three affiliates, we write in support of the "Improving Public Access to Documents Act of 2008." We commend Representative Jane Harman for taking this important step toward creating a more accountable government by compelling the Department of Homeland Security to develop policies and programs that limit and regulate the Federal government's use of control markings on unclassified documents. This important bill makes clear that controlled unclassified information (CUI) can be shared with State, local, and tribal governments, the private sector, and the public, as appropriate.

As the findings in the bill indicate, the proliferation of "sensitive but unclassified" (SBU) control markings interferes with accurate, actionable and timely information sharing, unnecessarily increases costs, and needlessly limits public access to information. The ACLU has long been concerned about the unregulated use of SBU markings, and any legislation that establishes a legal framework for controlling unclassified information must be drafted carefully to insure that it does not inadvertently create a secondary classification system that further restricts the public's access to information that does not meet the requirements necessary for classification.

The Improving Public Access to Documents Act of 2008 accomplishes this feat by requiring the Secretary of the Department of Homeland Security to develop CUI policies "in order to maximize the disclosure to the public." The bill includes critically important provisions establishing that CUI markings are not a determinant of public disclosure pursuant to the Freedom of Information Act and ensuring public access to unclassified information, even if marked CUI, under an appropriate FOIA request. 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.

Requiring the DHS Secretary to coordinate and consult with the Archivist of the National Archives and Records Administration, representatives of State, local and tribal governments, as well as civil liberties and government oversight organizations and the private sector will ensure that all stakeholders have a say in the development of these DHS policies and procedures.

We commend you for drafting a bill that encourages transparency in government and requires implementation of policies to maximize sharing of documents with the public.

Again, we thank you and your staffs for your open consultation with us with respect to your draft legislation. We look forward to working with you on this bill as it moves through the legislative process.

Sincerely,

Michael W. Macleod-Ball
Chief Legislative and Policy Counsel

Michael German
Policy Counsel

Timothy Sparapani
Senior Legislative Counsel

Ms. HARMAN. I would now ask Ms. Fuchs to summarize her statement for 5 minutes. I would point out that there is a little clock that will start ticking off the time. When it starts blinking red, please conclude.

STATEMENT OF MEREDITH FUCHS, GENERAL COUNSEL, NATIONAL SECURITY ARCHIVE

Ms. FUCHS. Thank you. Good morning, Chairwoman Harman and Mr. Reichert. Thank you for this opportunity to testify about the "Improving Public Access to Documents Act of 2008."

I represent the National Security Archive, a nongovernmental research institute at George Washington University. The archive conducted a governmentwide comparison of "sensitive but unclassified" control-labeled policies in 2006, and we concluded that the SBU practices of agencies could interfere with information-sharing and be abused for administrative convenience or to cover up information.

As the leading nonprofit user of the Freedom of Information Act and other programs designed to release information, the Archive is

concerned about the impending implementation of the Controlled Unclassified Information Framework that is described in the President's May 9 memorandum. I will call it the CUI framework for short.

I submitted written comments for the record, and this subcommittee is already well aware of the dangerous impact of the proliferation of "sensitive but unclassified" record control labels both on information-sharing and public disclosure. So in my summary statement today, I would like to focus only on a couple of key points.

First, the CUI framework perpetuates and extends a system of information control that has been abused in the past and left us vulnerable to harm in the past. While the establishment of trusted pathways for information is obviously essential to coordination amongst Federal, State, local and tribal governments and private parties, those pathways are susceptible to manipulation and failure, just as individual agencies that jealously guard their secrets and turf.

True information-sharing is best accomplished by the elimination of unnecessary secrecy and the minimization of information controls. The perspective adopted in the CUI framework, that the public should be left out of homeland security and terrorism matters, ignores the reality that the public will be affected by any attacks, has an interest in preventing attacks, and needs information to protect their families when first preventers and first responders are unavailable.

Think about the crime reports that most of us receive in our communities. When we learn that our community is being targeted, we can take measures to protect ourselves. In other words, sometimes information should be made available to the public not because of a Freedom of Information Act requests but simply because the public needs it. I hope this CUI framework does not lead to situations where such information is withheld or delayed because of a fear that it should stay secret. Thus, the provision in this bill requiring DHS to consult with public interest organizations helps bring the public back into the recognized stakeholder community.

Although this CUI framework itself has laudable and important goals, it does not include measures to reduce information control labelling and secrecy. Several of the provisions of H.R. 6193 that are designed to discourage unnecessary labelling are much-needed. We hope they are included in the National Archives implementing regulations for the CUI framework.

In particular, the establishment of a system for employee challenges to improper labelling, including incentives and rewards for challenges, is an internal check on abuse. The requirement that a list be maintained and available of records with CUI labels and the provision for Inspector General audits will remind information controllers that their decisions are subject to review. In addition, limiting the number of controllers will ensure that those who are granted the authority to put a CUI label on a record can be better trained and supervised.

I suggest one other measure be considered. The CUI framework does not provide any substantive definition of CUI. It merely is information pertinent to U.S. national interests or other important

interests that requires protection. That is a broad description, and it is eventually going to be defined within each agency based on the type of information that agency handles.

Agencies will be far more likely to define categories of CUI in a narrow fashion if their designations are subject to public review and comment. Accordingly, I recommend that DHS be required to provide transparency as it developed its substantive criteria for a CUI label.

My second concern—and I am going to close with this one—is that the CUI framework will have an impact on FOIA decision-making. The CUI label, in fact, should not really inform or otherwise influence FOIA release decisions. This bill is helpful for making that clear.

The CUI label has no duration. It does not recognize changes in factual circumstances. It doesn't consider a FOIA requester's identity or their reason for requesting the record or changes in FOIA policy concerning discretionary release of information. There is no basis in FOIA for any other statute to add as a new criterion a CUI label.

Each of those items I talked about are things that are considered in FOIA release decisions, and with the CUI label being considered, it could wait against release.

I spelled out more details in my written statement about this, and I will not repeat them now, other than to urge you to make the legislative history on this point clear: CUI should not have an impact on FOIA.

This bill provides protection against abuse of the new CUI framework and would make the framework work better. I do hope that it will be adopted Government-wide. I thank you for permitting me to testify, and I am happy to respond to your questions.

[The statement of Ms. Fuchs follows:]

PREPARED STATEMENT OF MEREDITH FUCHS

JUNE 11, 2008

Thank you Chairwoman Harman, Mr. Reichert, and Members of the subcommittee for this opportunity to comment on the "Improving Public Access to Documents Act of 2008."

I represent the National Security Archive, a non-governmental research institute at George Washington University. The Archive is one of the leading non-profit users of the Freedom of Information Act (FOIA) and the mandatory declassification review process, and relies on releases of government records to document important U.S. foreign relations, national security, and intelligence policy matters in our many publications.

In 2006 the Archive issued a report entitled: "Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive but Unclassified Information," which was the first Government-wide comparison of the ways that Federal agencies mark and protect unclassified, but sensitive, materials.[1] That report identified 28 different and uncoordinated control marking policies with no system to monitor or report on the use of control markings, no challenge or appeal mechanism to remove such markings, no "sunset" for the duration of most markings, few limits on who is authorized to put a control marking on material, and few limits on improper labeling of materials. The Archive's Director Tom Blanton testified before the Subcommittee on Emerging Threats of the House of Representatives Committee on Government Reform that the report concluded that neither the Congress nor the

[1] National Security Archive, "Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive but Unclassified Information," (March 14, 2006), available at *http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/press.htm.*

public could conclude whether the sensitive but unclassified policies were working to safeguard security or being abused for administrative convenience or cover-up. Indeed one of the government witnesses at that hearing acknowledged that there was no way to count or estimate the frequency of use of control markings.

I thank the subcommittee for its efforts to improve interagency information sharing and to simultaneously protect the public's access to government information. History teaches us that government secrecy is a natural bureaucratic tendency, although it is often intensified during times of perceived danger. As the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission") found, prior to the September 11, 2001, attacks on our Nation, the Government's intelligence and law enforcement communities too often controlled information to the detriment of effective security. In reaction to those attacks, agencies developed new forms of secrecy out of concern that sensitive information could reach the wrong hands, thus perpetuating the same problem that left the United States vulnerable to attack. It is against that background that Congress directed the President in the Intelligence Reform and Terrorism Prevention Act of 2004 to create an Information Sharing Environment that facilitates the sharing of terrorism information. While there are reflexive actions such as a short-term reduction in information disclosure that can be expected in the wake of a tragedy like the 9/11 attacks, the multi-year and multi-stakeholder process of developing the ISE had the benefit of resources and broad stakeholder input to reach a better balancing of all the relevant public interests.

The President's long-awaited Memorandum for the Heads of Executive Departments and Agencies on the Sharing of Controlled Unclassified Information (May 9, 2008) (the "Presidential Memorandum") and the CUI Framework, which is the name being given to the policies and procedures that govern handling of what will now be called Controlled Unclassified Information (CUI), are responsive to some of the concerns that open government advocates have expressed about the proliferation of varied categories of sensitive but unclassified information.

Thus, over time, the Framework should reduce the over 100 different record control labels used throughout the Federal Government down to three primary labels with limits on the unnecessary expansion of that number of labels. The procedures for handling materials marked with the new labels set forth under the CUI Framework will be uniform across agencies. If properly implemented, the CUI Framework should undoubtedly improve the ability of agencies to share information with other agencies, as well as State, local, and tribal officials, and other parties. Further, the Framework should make it easier for members of the public to understand the significance of CUI labels so that the labeling of records may not appear as arbitrary and inappropriate as it has in the past.

On the other hand, many of the most critical concerns of the open government community are not specifically addressed in the CUI Framework. I would like to address two broad concerns and discuss how the "Improving Public Access to Documents Act of 2008" (H.R. 6193) would have an impact on these concerns. I also hope that many of these issues will be addressed in the implementing regulations of the Executive Agent of the CUI Framework, the National Archives and Records Administration (NARA), as this bill would apply only to the Department of Homeland Security.

THE PROBLEM OF UNNECESSARY CONTROL LABELING OF MATERIALS

The CUI Framework focuses on standardization of CUI practices without sufficient attention to the need to reduce unnecessary protection of information. For example, in its statement of purpose, the Presidential Memorandum makes no mention of reducing the use of CUI-type labeling.

True information sharing is best accomplished by the elimination of unnecessary secrecy and information controls. We know well from the security classification realm that too much information is made secret when there are no incentives to reduce secrecy. In the classified area, authorities typically protect classifiable information (and sometimes information that does not even merit classification) without any consideration of the costs to national security or to the public interest incurred by the classification. Indeed, numerous high level Government officials from then-Secretary of Defense Donald Rumsfeld,[2] to then-Chair of the House Permanent Select Committee on Intelligence Porter Goss,[3] to the Deputy Secretary of Defense for

[2] Donald Rumsfeld, *War of the Worlds,* Wall St. J., July 18, 2005, at A12 ("I have long believed that too much material is classified across the Federal Government as a general rule . . .").

[3] *9/11 Commission Hearing,* (Testimony of then Chair of the House Permanent Select Committee on Intelligence Porter Goss) (2003), *http://www.9-11commission.gov/archive/hearing2/*

Counterintelligence and Security,[4] have recognized that a tremendous amount of information is improperly and unnecessarily classified. The cost of such over-classification also has been acknowledged within Government. Overclassification interferes with information sharing, breeds contempt for the security classification system, is undemocratic, and unnecessarily expends taxpayer funds.

CUI certainly is vulnerable to the same unnecessary secrecy. Currently, all records within an agency may receive an FOUO (for official use only) or OUO (official use only) label simply because the record is an official government record. The CUI Framework sketched out in the Presidential Memorandum does not confront this problem directly. It provides only the barest explanation of what can substantively be called CUI: information that is "pertinent" to U.S. national interests or "important interests" of other entities and "requires protection." President's Memorandum § 3(a). Thus, CUI is an easily expandable concept.

There are, however, some touchstones in the President's Memorandum to support additional measures to reduce unnecessary control labeling. The Memorandum provides for portion marking where feasible, rather than the marking of complete documents when the material contains both CUI and non-CUI. Id. § 15. It also provides that information should not be labeled as CUI for an improper purpose. Id. § 26. The Presidential Memorandum further provides that if information is required to be made public or has already been released then it may not be labeled CUI and that non-CUI should not be subject to handling and dissemination controls. Id. §§ 18 and 26. The Background on the Controlled Unclassified Information Framework (May 20, 2008) provides further support, as it recognizes the goal of "control[ling] only information that should be controlled."[5]

None of those provisions, however, directly counteract the many incentives to insert a control marking on a government record. For example, there are enforcement mechanisms and penalties built in to the CUI framework, id. § 22(i) and 24(g), that fail to mention the possibility that they would apply to improper or unnecessary labeling. H.R. 6193 adds several additional requirements with respect to the Department of Homeland Security's CUI program that may, if enacted into law and implemented, be far more likely than the Presidential Memorandum to reduce the labeling of records as CUI.

First, H.R. 6193 recognizes that the harmful impacts of excessive secrecy include interference with inter-agency information sharing, as well as increased costs of information security and obstacles to the release of information to the public. H.R. 6193, Findings § 2(1). Those findings provide a critical context for the CUI Framework because they encourage the Department to move away from the flawed and dangerous "secrecy equals security" paradigm. When considered in conjunction with the instruction to the Secretary of Homeland Security to implement the CUI Framework in a manner that would "maximize the disclosure to the public" of information and to consult with "organizations with expertise in civil liberties, civil rights, and government oversight," id. § 3 (210F(a)), the bill should encourage consideration of the costs of secrecy and of the benefits of disclosure, which are too often absent from government disclosure decisionmaking. Moreover, the requirement that DHS consult with public interest, non-governmental organizations recognizes the reality that members of the public are stakeholders who care about the effectiveness of the CUI Framework and about protecting important rights.

Second, the establishment of a system that permits employee challenges to the use of CUI markings and rewards appropriate use of the challenge procedure will put in an internal check on abuses of the CUI labeling framework at the Department. This is a necessary counterbalance to the incentives included in the Presidential Memorandum to err on the side of marking information as CUI, such as the

---

9-11Commission__Hearing__2003-05-22.htm#panel__two ("[W]e overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them.").

[4] *Subcommittee on National Security, Emerging Threats and International Relations of the House Committee on Gov't Reform Hearing,* 108th Cong. (2004) (testimony of Carol A. Haave), *http://www.fas.org/sgp/congress/2004/082404transcript.pdf* (stating under repeated questioning from Members of Congress that approximately 50 percent of classification decisions are over-classifications).

[5] Indeed, we are pleased that the Archivist of the United States, as the head of the Executive Agent NARA, has directed the office that will implement the framework "to ensure that only information which genuinely requires the protections afforded by the President's memorandum will be introduced into the CUI Framework." NARA Press Release (May 22, 2008); see also Memorandum of Allen Weinstein, Archivist of the United States to the Executive Department and Agencies on the Establishment of the Controlled Unclassified Information Office (May 21, 2008). We hope that NARA's implementing regulations will include this goal and will include many of the good ideas included in H.R. 6193 to help accomplish this goal across the entire Federal Government.

enforcement and penalty provisions and the requirement that disclosure of CUI be reported to the originating agency. The internal check on over-controlling information could be substantially strengthened by a specific requirement that the Inspector General audits of the CUI program assess the extent that the control labels are used unnecessarily or excessively.

Third, the legislation provides for a publicly available list of materials marked as CUI that notes whether they have been withheld under the FOIA and a process for the public to challenge such CUI markings. Importantly, this requirement will discourage thoughtless use of the CUI stamp. Personnel with authority to label records as controlled will take a moment to consider whether the label is necessary if they know that their decision will be tracked and reviewable.

Fourth, the bill's requirement that the Department limit the number of people who can put a control stamp on materials will decrease the unnecessary labeling of materials. The Archive's 2006 study determined that the Department of Homeland Security permits any employee to designate sensitive unclassified information for protection. Under the bill, the Department would have to limit the individuals with authority to use control markings and ensure they are properly trained in the appropriate use of such markings.

In addition to these many useful limits on the expansion of CUI, we recommend that the bill require the Department to provide transparency regarding any new directives, regulations, or guidance promulgated pursuant to the Presidential Memorandum and provided to the Executive Agent that relate to the substantive description of what will be labeled as CUI within the Department. Public notice and comment regarding the definition of CUI at DHS will increase the likelihood that such measures would be narrowly tailored.

IMPACT ON THE FREEDOM OF INFORMATION ACT

My second major area of comment is the need to build in mechanisms to discourage agencies from treating CUI labels as de facto determinations of FOIA exemption. Prior to the issuance of the Presidential Memorandum, agencies were split as to whether SBU labels were relevant to FOIA determinations. Some agencies only labeled records as SBU if a FOIA exemption applied. Others claimed SBU had nothing to do with FOIA. The Memorandum says that a control label "may inform but do[es] not control" the decision whether to disclose information under the FOIA. There are several problems with this formulation.

First, the applicability of FOIA exemptions changes over time. For example, a record classified under Executive Order 12958 one day may be declassified a year later.[6] Similarly, a law enforcement investigation may end, rendering records about the investigation newly releasable. Yet, CUI control labels do not have expiration dates or take account of changing circumstances.

Second, FOIA policy changes over time, as illustrated by the different policy memoranda issued by Attorney General Reno and Attorney General Ashcroft.[7] Thus, Government agencies may change their policy with respect to making discretionary releases under the FOIA and the CUI label will not incorporate any consideration of these policy changes.

Third, the identity of the requester and the reason for the request may affect the releasability of the record under FOIA. For example, in cases raising privacy issues, the identity of the requester may affect whether an agency would conclude that there is a "clearly unwarranted invasion of privacy" under Exemption 6 or an "unwarranted invasion of privacy" under Exemption 7(C) of the FOIA. 5 U.S.C. §§ 552(b)(6) and (b)(7)(C). The purpose for which the record is sought also is relevant under the privacy exemptions because it informs the evaluation of the public interest served by the requested release.

For all of these reasons, any consideration of a CUI label in the FOIA process presents a true risk that the label may weight disclosure decisions against disclosure even when the FOIA exemptions would no longer apply.

H.R. 6193 would encourage the Department to base its disclosure decisions on the presumption that its records are public absent a legitimate reason not to disclose the record. This perspective properly places the burden on the Department to justify non-disclosure, rather than on the public to justify why a record should not be withheld. The most critical parts of the bill are the provision that "controlled unclassified information markings are not a determinant of public disclosure pursuant to

[6] See Exec. Order No. 12,958 (as amended by Exec. Order No. 13,292), 68 Fed. Reg. 15315 (Mar. 25, 2003).

[7] See New Attorney General FOIA Memorandum Issued, FOIA Post (Department of Justice, Washington, DC), Oct. 15, 2001, *http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.*

[the FOIA]," H.R. 6193 § 3 (210F(c)(3)(D)) and the provision which provides that the Secretary make available to the public under FOIA "all controlled unclassified information and other unclassified information in its possession." Id. § 3 (Section 210F(d)).

The existing standards in the classification system and the FOIA system for disclosure are sufficiently broad to address the need to protect sensitive information. They apply Government-wide and are not subject to the whims of a particular agency. That will not be the case with CUI, which will be substantively defined by each agency within its discretion. There is no congressional or Presidential mandate to label any particular records as CUI. It is, at best, an administrative management measure by agencies to help them communicated better with each other. Further, as mentioned above, the FOIA standards recognize the expiration of sensitivities, while the CUI Framework does not. Without the two provisions barring the CUI Framework from having an impact on FOIA disclosure the bill will have only a negligible impact on preservation of the public right to know.

Indeed, I recommend the subcommittee consider going even further to ensure that FOIA disclosure is not impacted by the CUI Framework. Although the Presidential Memorandum makes clear that CUI is not intended to act as a security classification standard,[8] the systematization of the CUI Framework may elevate the status of the previously disorganized SBU system for agencies, Congress, and the courts. I recommend adding a clear statement that the CUI label does not warrant judicial deference relating to public disclosure of materials. As noted above, the substantive requirements for a CUI label will be decided by each agency pursuant to its own perspective. There is no basis for a court to defer on the question of whether a CUI record is properly withheld from the public. Courts should continue to look to the well-established standards of the Executive Order on Classification, EO 12958, as amended, and the FOIA.

Thank you for the opportunity to testify. I would be happy to respond to your questions.

Ms. HARMAN. Thank you very much.

Ms. McDermott, please summarize your statement in 5 minutes.

STATEMENT OF PATRICE MCDERMOTT, DIRECTOR, OPENTHEGOVERNMENT.ORG

Ms. MCDERMOTT. Thank you. Good morning. Thank you, Chairwoman Harman and Mr. Reichert, for the opportunity to speak today on the proposed legislation.

In March 1972, speaking about his executive order on national security classification, President Richard Nixon noted 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." He had it right then, and it is still true now.

A month ago, as you know, the White House issued a memorandum to all heads of executive departments and agencies that intends 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.

I would like to make three points about the implementation of that memorandum, with the focus on your legislation to direct how it is implemented at the Department of Homeland Security.

---

[8] Presidential Memorandum § 1 ("The memorandum's purpose . . . [is] not to classify or declassify new or additional information"); id. § 3(a) (CUI is unclassified information that "does not meet the standards for National Security Classification under Executive Order 12958, as amended").

First of all, the default must be openness. We are very pleased that you have designated your legislation as the "Improving Public Access to Documents Act," although, as you know, the name alone will not determine the reality.

As noted 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 that 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 CUI.

The default bureaucratic position is to not take risk. Unfortunately that message has been given to officials in our government, that openness is risky. This is not only a dangerous mindset in an open society, but, as you 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 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.

To counter the impulse toward nondisclosure, the bill has three provisions 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 of these establishes that CUI markings are not a determinant of public disclosure pursuant to FOIA. As I noted in my submitted written testimony, a 2006 GAO report clearly indicated that agencies think of the several FOIA exemptions, the current FOIA exemptions, as creating control categories. They consider them CUI. The effect on access to information through FOIA has been pernicious.

To ensure that this provision is properly implemented, the legislation contains two critically important requirements: to maintain a publicly available list of documents designated and marked in whole or part as CUI and indicating which have been withheld in response to a request; and to create a process through which the public may seek the removal of such a designation and marking. Both of those are entirely absent in the White House framework.

This list of documents is essential not only for ensuring that CUI markings do not preclude disclosure under FOIA but as a critical tool for oversight and for maintaining a check on agencies' demonstrated impulse to overcontrol and overdesignate information.

From our perspective, the focus on FOIA, while critical, should not obscure that this is a fallback channel for public access to agency information on homeland security and related topics. If disclosure under FOIA is seen as the primary alternative to classification

or control, an impossible burden may be placed on the FOIA process.

The second key set of provisions concerns controlling the controllers. Ms. Fuchs has addressed some of these. The tracking of employees' markings and use and the ability and the requirement that the Department consult with outsiders, with other stakeholders, and also that this plays a role in determining how many people have designation authority.

We also urge you to protect throughout the legislative process, as Ms. Fuchs noted, the inclusion of outside groups, public interest groups, because these help to promote trust and accountability.

Third, information sharing must include the public. We have experienced a trend in our country away from trusting the public to a need-to-know mindset. We need to move away from that, and this legislation takes an important step toward doing that.

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 is truly improved.

Thank you again for this opportunity, and I would be pleased to answer any questions.

[The statement of Ms. McDermott follows:]

PREPARED STATEMENT OF PATRICE MCDERMOTT

JUNE 11, 2008

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.

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

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

[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.*

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.

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.

---

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

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 governmentwide 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" mindset. 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 ex-

cluded. 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.

Ms. HARMAN. Thank you very much.

Ms. Fredrickson, please summarize your testimony in 5 minutes.

STATEMENT OF CAROLINE FREDRICKSON, DIRECTOR, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION

Ms. FREDRICKSON. Good morning, Chair Harman, Ranking Member Reichert, Members of the subcommittee.

Thank you so much for this opportunity to testify on behalf of the American Civil Liberties Union about an issue of critical importance to all Americans, the right of the people to know what our Government is doing. I also would say I appreciate very much the opportunity to testify with such a distinguished panel.

We testified today in support of the "Improving Public Access to Documents Act of 2008," which would create a more accountable government by compelling the Department of Homeland Security to develop policies to limit and regulate the Federal Government's use of control markings on unclassified documents. This important bill makes clear that controlled unclassified information, or CUI, can be shared with State, local and tribal governments, the private sector and the public, as appropriate.

Our Nation has often faced grave threats to our security but has recognized that abandoning our fundamental democratic principles does not make us stronger. During the height of the Cold War, President John F. Kennedy said, "The very word 'secrecy' is repugnant in a free and open society." We decided long ago that the dangers of excessive and unwarranted concealment of pertinent facts far outweighed the dangers which are cited to justify it.

Despite the near-universal recognition that the failure to effectively share information was a contributing factor in the intelligence breakdowns that led to 9/11, Government agencies have increasingly been using unregulated control designations that restrict the free flow of information and increase confusion regarding what information may be shared, with whom and how.

Testimony before this subcommittee last year revealed that 20 Federal agencies use at least 107 different control markings. All

[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.*

the information subject to these 107 unregulated control markings is, by law, unclassified. Federal agencies began using control markings on unclassified documents they considered sensitive in the 1970's, but the term "sensitive but unclassified," or SBU, has never been defined in statutory law.

Last month the White House issued a memorandum that adopts CUI as the sole SBU—excuse me for the acronyms—designation for the Federal Government. The executive order seeks to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information.

The ACLU has grave concerns that once a CUI framework is developed, officials could ignore this lofty purpose and use CUI markings to improperly withhold unclassified documents from public disclosure. That is why legislative guidance is so necessary to ensure that Government officials use CUI markings to increase information-sharing rather than restrict it.

Any legislation that establishes a legal framework for controlling unclassified information must be drafted carefully to ensure that it does not inadvertently create a secondary classification system that further restricts the public's access to information. The "Improving Public Access to Documents Act" accomplishes this feat by requiring the Secretary of the Department of Homeland Security to develop CUI policies, quote, "in order to maximize the disclosure to the public."

Requiring DHS to coordinate and consult with the archivist of the National Archives, State, local and tribal governments, as well as civil liberties organizations and the private sector, will ensure that all stakeholders have a say in the development of these DHS policies and procedures.

Congress recognized the public's right to information held by our Government when it passed the Freedom of Information Act in 1966 and voted to strengthen it in 1974, 1976, 1986, 1996, and again last year.

Your bill includes two critically important provisions: Establishing that CUI markings are not allowed to undermine FOIA; and ensuring public access to unclassified information even if marked CUI under an appropriate FOIA request. These must be included in any legislation that may be signed into law.

The bill properly limits what types of information may be designated CUI and prohibits use of CUI markings to conceal violations of law or prevent embarrassment to an agency.

The bill includes many other important provisions that my colleagues have mentioned already, so I will conclude by saying that we are very happy to support the "Improving Public Access to Documents Act of 2008" and look forward to working with you to see it moved to statute with all of its provisions intact.

Thank you.

[The statement of Ms. Fredrickson follows:]

PREPARED STATEMENT OF CAROLINE FREDRICKSON

JUNE 11, 2008

Good morning Chair Harman, Ranking Member Reichert, and Members of the subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union, its hundreds of thousands of members and 53 affiliates Na-

tion-wide, about an issue of critical importance to all Americans: the right of the people to know what our Government is doing and to have access to documents created at taxpayer expense. As this committee knows, excessive government secrecy harms our national security and undermines our democratic institutions. Secrecy interferes with the timely sharing of accurate and actionable information, unnecessarily increases government costs, and frustrates democratic accountability by improperly limiting public access to information.

We testify today in support of the "Improving Public Access to Documents Act of 2008," which is an important step toward creating a more accountable government by compelling the Department of Homeland Security to develop policies and programs that limit and regulate the Federal Government's use of control markings on unclassified documents. This important bill makes clear that controlled unclassified information (CUI) can be shared with State, local, and tribal governments, the private sector, and the public, as appropriate.

THE NEED FOR LEGISLATION TO REDUCE UNNECESSARY GOVERNMENT SECRECY

Our Nation has often faced grave threats to our security, but abandoning our fundamental democratic principles to address those threats does not make us stronger. During the height of the Cold War President John F. Kennedy said,

"The very word 'secrecy' is repugnant in a free and open society; and we are as a people inherently and historically opposed to secret societies, to secret oaths and to secret proceedings. We decided long ago that the dangers of excessive and unwarranted concealment of pertinent facts far outweighed the dangers which are cited to justify it. Even today, there is little value in opposing the threat of a closed society by imitating its arbitrary restrictions. Even today, there is little value in insuring the survival of our Nation if our traditions do not survive with it."[1]

Despite the near-universal recognition that the failure to effectively share information was a contributing factor in the intelligence breakdowns that led to 9/11, Government agencies have been increasingly using a multitude of unregulated control designations that restrict the free flow of information and increase confusion among agencies regarding what information may be shared, with whom, and how. The improper use of control markings can forestall the sharing of critical information with State, local and tribal law enforcement officials making it all the more difficult for local law enforcement to know the vulnerabilities in their own communities.

In testimony before this subcommittee last year, Ambassador Ted McNamara, Program Manager of the Director of National Intelligence Information Sharing Environment, revealed that 20 Federal Government departments and agencies use at least 107 different control markings with more than 131 different procedures for handling what those agencies considered "sensitive" information.[2] McNamara concluded, not surprisingly, that the confusion over how information marked with a particular control designation should be handled reduced information sharing. What should be shocking to the American public, however, is that all the information subject to these 107 unregulated control markings is, by law, unclassified. According to the Congressional Research Service, Federal agencies began using control markings on unclassified documents they considered "sensitive" in the 1970's, but the term "sensitive but unclassified" (SBU) has never been defined in statutory law.[3]

The Government regulates the disclosure of "national security information" through a classification system established in Executive Order 12958, as amended. "National security information" subject to classification under the executive order is defined through extraordinarily broad categories of information:

- military plans, weapon systems, or operations;
- foreign government information;
- intelligence activities, sources and methods, or cryptology;

---

[1] John F. Kennedy, Address Before the American Newspaper Publisher's Association, New York, NY, (Apr. 1, 1961), available at *http://www.jfklibrary.org/Historical+Resources/Archives/Reference+Desk/Speeches/JFK/003POF03NewspaperPublishers04271961.htm.*

[2] *The Over-Classification and Pseudo-Classification of Governmental Information: The Response of the Program Manager of the Information Sharing Environment: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment H. Committee on Homeland Security,* 110th Cong. (Apr. 26, 2007) (Statement of Ambassador Ted McNamara, Program Manager, Information Sharing Environment), available at *http://homeland.house.gov/SiteDocuments/20070427081925-82568.pdf.*

[3] Genevieve J. Knezo, SENSITIVE BUT UNCLASSIFIED INFORMATION AND OTHER CONTROLS: POLICY OPTIONS FOR SCIENTIFIC AND TECHNICAL INFORMATION, CRS Report for Congress (Dec. 29, 2006), available at *http://www.fas.org/sgp/crs/secrecy/RL33303.pdf.*

- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic information related to the national security;
- U.S. programs for safeguarding nuclear material and facilities;
- vulnerabilities and capabilities of U.S. systems, installations, infrastructure, projects, plans or protection services related to the national security; and
- weapons of mass destruction.[4]

By definition, any information designated SBU falls outside these broad categories, so any national security argument for restricting the distribution of SBU information is greatly diminished.

Moreover, the problem with the unrestricted use of SBU markings by Government agencies is not limited to impeding effective sharing of intelligence information among Federal agencies and their partners in State, local and tribal government. The unchecked ability to shield government documents from disclosure encourages agencies to hide their mistakes and thwarts effective oversight. The Director of the Defense Capabilities and Management at the Government Accountability Office (GAO), Davi M. D'Agostino, studied how the Departments of Energy and Defense handled CUI and noted:

" . . . neither Departments' policies identify what would be an inappropriate use of the FOUO [For Official Use Only] or OUO [Official Use Only] designation. Without such guidance, the Departments cannot be confident that their personnel will not use these markings to conceal mismanagement, inefficiencies, or administrative errors, or to prevent embarrassment."[5]

SBU designations have even been used to obstruct congressional oversight. Representative Henry Waxman, Chairman of the House Government Reform and Oversight Committee, noted in 2006:

"Last year, Chairman Shays and I sought documents from three agencies, the Defense Department, State Department, and the Department of Homeland Security, that had been restricted as 'Sensitive But Unclassified' or 'For Official Use Only.' To date, we have received none of these documents. It is particularly telling that in their responses, the agencies claimed they had no way to provide such information because they don't keep track of it. As another agency wrote, there is no regulatory or other national policy governing the use of 'For Official Use Only,' this designation, as opposed to the controls on classified national security information."[6]

Last month the White House issued a memorandum to the heads of all executive branch agencies that adopts "Controlled Unclassified Information" (CUI) as the sole SBU designation for the Federal Government and establishes a framework for its use. The stated purpose of this executive order is "to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information."[7] The ACLU has grave concerns that once a CUI framework is developed executive branch officials could ignore this lofty purpose and use CUI markings to improperly withhold unclassified documents from public disclosure, much the way the classification system is currently over-used and abused. Providing legislative guidance is both necessary and appropriate to ensure that executive branch officials use CUI markings in the manner intended, to increase information sharing rather than to restrict it.

Congress recognized the public's right to information held by our Government when it passed the Freedom of Information Act in 1966, and voted to strengthen it in 1974, 1976, 1986, 1996, and again last year. FOIA exemptions permit the government to withhold information that is properly classified for national security or law enforcement purposes; trade secrets and privileged and confidential commercial

---

[4] Exec. Order No. 13,292, amending Exec. Order No. 12,958, (Mar. 25, 2003), available at *http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html.*

[5] *Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the H. Committee on Government Reform,* 109th Cong. 243 (2006) (Statement of Davi M. D'Agostino Director of the Defense Capabilities and Management at the Government Accountability Office (GAO)).

[6] *Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the H. Committee on Government Reform,* 109th Cong. 8–9 (2006) (Statement of Rep. Waxman, Ranking Member, H. Comm. on Government Reform).

[7] Memorandum from George W. Bush to the Heads of Executive Departments and Agencies, "Designation and Sharing of Controlled Unclassified Information", May 9, 2008, *http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html.*

or financial information; interagency deliberations; and personnel files requiring privacy, among other types of information. By creating these broad exemptions Congress has already established a process for limiting disclosure of information that might harm the national security or some other important Government or private interest. CUI markings should never be allowed to undermine FOIA and interfere with the public's right to know.

FEDERAL AGENCIES NEED CONSISTENT STANDARDS AND STATUTORY GUIDANCE TO LIMIT THE USE OF CUI DESIGNATIONS AND ENSURE APPROPRIATE PUBLIC ACCESS TO UNCLASSIFIED INFORMATION

As the findings in the Improving Public Access to Documents Act of 2008 indicate, the proliferation of SBU control markings interferes with accurate, actionable and timely information sharing, unnecessarily increases costs, and needlessly limits public access to information. The finding acknowledging the negative impact the overuse of control markings has on our national security is crucial to correcting the trend toward secrecy that, as the bill states, is antithetical to the concept of an information sharing environment.

The ACLU has long been concerned about the unregulated use of SBU markings, and any legislation that establishes a legal framework for controlling unclassified information must be drafted carefully to insure that it does not inadvertently create a secondary classification system that further restricts the public's access to information inappropriately. The Improving Public Access to Documents Act of 2008 accomplishes this feat by requiring the Secretary of the Department of Homeland Security to develop CUI policies "in order to maximize the disclosure to the public." Requiring the DHS Secretary to coordinate and consult with the Archivist of the National Archives and Records Administration, representatives of State, local and tribal governments, as well as civil liberties and Government oversight organizations and the private sector will ensure that all stakeholders have a say in the development of these DHS policies and procedures.

The bill includes two critically important provisions establishing that CUI markings are not a determinant of public disclosure pursuant to FOIA and ensuring public access to unclassified information, even if marked CUI, under an appropriate FOIA request. 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 bill properly limits what types of information may be designated CUI, and prohibits use of CUI markings to conceal violations of law or prevent embarrassment to an agency. The bill also properly limits the number of employees who are authorized to make CUI markings, and establishes mechanisms to track their decisions and hold them responsible, which hopefully will change the current culture from need-to-know to need-to-share.

The bill includes other important elements that will ensure proper oversight of the implementation of the CUI framework, including an ongoing auditing mechanism administered by the DHS Inspector General that will assess whether CUI markings are being used properly, with a requirement for annual reporting to Congress. Establishing a reward process where employees can challenge CUI markings will also be helpful to limiting improper designations. And the requirement that DHS maintain a publicly available list of documents marked CUI that have been withheld under FOIA will increase public oversight, and hopefully will compel more thorough deliberation when marking or withholding requested documents.

CONCLUSION

Without a legal framework, Federal agencies' use of SBU control markings can intentionally or inadvertently obscure critical information from the public as well as from State, local, and tribal law enforcement. The Improving Public Access to Documents Act of 2008 would enhance information sharing with State, local, and tribal governments by requiring a more uniform standard for handling CUI and alleviating confusion about what information can be shared. Definitive statements that CUI markings are not a determinant of public disclosure under FOIA will ensure that the purpose of this bill is realized by improving public access to documents. We are happy to support the Improving Public Access to Documents Act of 2008 and look forward to working with you to protect its most essential provisions as it moves through the legislative process.

Ms. HARMAN. Thank you, Ms. Fredrickson.

I thank all the witnesses for observing the time limits, and welcome three more members who are here to ask questions. They will

be recognized in the order that they arrived after the Ranking Member and I ask our own questions.

I now yield myself 5 minutes for questions.

Everyone probably already knows the formal name of this subcommittee is Intelligence, Information Sharing and Terrorism Risk Assessment. Information sharing, all of us believe, is an absolute key to getting and sharing intelligence with those who need to know it. So we have been hammering on Government agencies and others, for the better part of 2 years, to break down old cultures.

One of you mentioned the need-to-know culture, which is still sadly alive. It must change to a need-to-share culture. That is certainly a premise that underlies a lot of the work we have been trying to do here. I am pleased to hear that all of you support the work that we are doing on this legislation.

Let me just ask two questions because I want to spend some time on others.

No. 1, as I made clear in my opening remarks, we are trying to make DHS the gold standard with respect to implementing these new guidelines. We are doing that for two reasons. One, we think that DHS has critical jurisdiction and is part of the problem and could change, should change for the better. But the second is, we have jurisdiction over DHS. That should be obvious.

One of you mentioned that this should be a Government-wide policy. I would just like to hear some more support for that position or your additional comments on that. That is the first thing.

The second thing, one of you said that a reason that many hide information or stamp information with protective categories is bureaucratic turf and power. I obviously agree with that, but I would like you to explain that.

Let me just add one thing to that. As a member of the House Intelligence Committee for 8 years, from 1996 with a little interruption until 2006, I came to respect enormously what I think is a good reason to protect information, and that is to protect sources and methods. People die if sources or methods are disclosed. Especially if, on an ongoing basis, we are trying to learn the plans and intentions of bad guys, we have to protect our sources and methods. But I never could find another good reason for protecting information. So I don't personally think that bureaucratic turf and power are good reasons. I would just welcome, again, some comments to fill out our record.

So both of those are my questions and my only questions. One is, should this approach that we are taking apply Government-wide? The second is, please explain your comments about bureaucratic turf and power. Let us know if you think there are any good reasons, other than protecting sources and methods, to hide information from the public.

Ms. Fuchs.

Ms. FUCHS. I would be happy to start off.

I think that the reason that the standards need to be applied Government-wide is that, while certainly DHS is critical in terms of the information-sharing environment, the reality is there are other agencies, law enforcement agencies, intelligence agencies that do participate in the information-sharing environment, and they all have similar problems to DHS.

The CUI framework that the President has established certainly provides some very positive aspects in order to increase information sharing, but it really doesn't provide protections against it being abused. I think that this bill includes many of those protections. Indeed, we hope to make similar comments as we have made today to the National Archives to let them know that we would like to see this in their implementing regulations if it does not become Government-wide statute.

Then simply to respond on the question about bureaucratic turf and power, I mean, we see examples again and again in the classification realm where information is improperly classified, and when you actually see the information, the only reason that you can identify the classification was because they were embarrassed or they didn't want people to know the position they are taking.

You know, a good current example is some of the memos that were written regarding torture and detention that were classified, and now that those memos, parts of them are being made public, it is clear that at least what was classified probably could have been made public.

My understanding is, for some of these memos that justified surveillance, you know, not even general counsels within Government agencies were allowed to look at those memos. That doesn't make any sense to me. To me, that is clearly about power and not the proper use of classification stamp.

Ms. HARMAN. Thank you.

Other comments?

Ms. MCDERMOTT. Well, I think I am the one who said that they tend to stand for bureaucratic turf and power. I know anecdotally—obviously, I am not inside the Government—but we heard in relation to the events of 9/11 that information was not shared. Unclassified information, even, was not shared.

We have seen in the GAO report that there is great difficulty across Government and from Government to other levels of Government in sharing information. It appears to be that it is about controlling information in order to keep it within the control of a particular bureaucracy, rather than letting it get out to other agencies who may do other things with it or may release it.

So I think this is a—from what GAO has reported and what we hear in the newspapers and what you have heard and released here in the Congress, this is a severe problem with control for its own sake and, also, control for avoidance of risk, which is the flip side of that.

We do agree that this—we would hope to the provisions in this bill do become Government-wide policy because, as I noted in my written testimony, there are many important provisions in here: the auditing, the tracking, the encouragement of people to challenge markings. We would add, as I do in my written testimony, that there need to be whistleblower protections for those people, as well.

But DHS is a poster child for nondisclosure and nontransparency, at the moment. If you can make DHS the gold standard, I would think that will set a very strong example. We also will be working with National Security Archives and our other partners in the coalition to encourage the National Archives, as they imple-

ment the White House framework, the CUI framework, to adopt some of these policies that are contained in your bill.

Ms. HARMAN. Thank you.

Ms. Fredrickson.

Ms. FREDRICKSON. I associate myself with the comments of my colleagues and only add one thing. I think, as Patrice rightly said, it is not simply bureaucratic turf battles and control and urge for power, but there is also a fear of risk. I think your legislation addresses that very well by limiting the number of individuals that actually can designate the documents as CUI and also makes them accountable. Having the list of documents published I think is a very important mechanism for ensuring that people don't, out of fear or risk-averse tendencies, decide to keep everything secret if they can. So thank you for that.

Ms. HARMAN. Thank you very much.

I am aware that the answers of witnesses went over my time limit, so I will afford other members the same courtesy.

Mr. Reichert.

Mr. REICHERT. You have that prerogative, Madam Chair.

I want to thank you again for being here today. A lot of things that all three of you said, it just kind of brought back flashes of my previous career and various things that we confronted, as far as information-sharing and withholding information.

I started in law enforcement back in 1972. Don't worry, I am not going to go through my whole career. But I did have dark brown hair, by the way, back then.

You know, there was a problem that when you worked—there were street crimes units who worked on street crime, which included a variety of crime, and then they worked with a drug unit that worked on drug crimes. There was an inability or an unwillingness, I should say, for those units to share information because there was a turf battle, and it persists today.

But you rise above the local competition there between two units within a police department or a sheriff's office, and now you are talking about sheriff's offices and police departments that don't share information between the two of them, or especially in the Green River case back in Seattle where many, many agencies were involved and there was a fear of sharing information because they would be tied to the investigation. The news media would be all over their backs, demanding, "What are you going to do to solve this case?" They wanted to stay out of it. I mean, they would just go on and on with the reasons. But I clearly understand this issue.

But I also want to point out that we have made great progress since those days. The fusion centers that exist today, the Joint Terrorism Task Force—there is this effort now for agencies to share information between themselves. But I agree with you, after September 11, as the sheriff in King County, we had struggled greatly with the Federal Government to share information with law enforcement leaders. I had 1,100 employees that needed to know certain things were happening, and we were not told. The police chief of Seattle will tell you that the same thing happened. The State patrol chief will tell you the same thing happened there.

So not only do the law enforcement agencies need to have that information, but I agree with you, the public does. In the fusion

centers, we have included people from the public, from various businesses and other public entities in the communities now are all a part of our fusion centers and sharing information.

I would like—you made a comment, Ms. Fredrickson, on the risk of fear. What do you exactly mean by—the fear of risk, I should say. What do you mean by that?

Ms. FREDRICKSON. Well, you know, I think it is commendable, and many law enforcement and in our government really want to keep us safe, and I think we all appreciate that. I think, though, there may not be an appreciation of the fact that sometimes, I think as Meredith said specifically, that it is actually providing of information that keeps us safe.

So, that is why it is very critical that I think we overcome some of what may seem to be risk-averse tendencies of people to keep things classified or keep them secret or keep them away from the public. That has very pernicious consequences when that information is not appropriately withheld.

Mr. REICHERT. Do you think there is a fear of lawsuits?

Ms. FREDRICKSON. There may be. That is really not what I was thinking of specifically.

Mr. REICHERT. One of the risks?

Ms. FREDRICKSON. I am thinking of their higher intentions, that there actually is a real desire to keep us safe but that sometimes it may be misleading, in the sense that it leads to actions that actually undermine our safety.

Mr. REICHERT. A question about FOIA requests. About how many requests do you think are made a week, if anybody on the panel would know? Do you know how many a week, a month? Or do you keep track of the number of requests made?

Ms. FUCHS. Yeah, Government-wide, there is something like 20 million—is that correct?

Ms. MCDERMOTT. Yeah, I think that is right.

Ms. FUCHS. But that includes privacy act requests, which are when people, you know, veterans ask for their own records. In terms of FOIA requests, it is probably a couple million each year. They are a wide range in terms of how complicated or not complicated they are.

Mr. REICHERT. Do you feel like you are getting prompt responses or——

Ms. FUCHS. No.

Mr. REICHERT. This is the response I expected, by the way.

Ms. HARMAN. I planted this question.

Ms. FUCHS. My organization, in fact, has done several studies looking at the oldest FOIA requests in Government, and, in fact, there are some that are 15, 18 years old. Of course, those are the hardest ones. As you know, there was legislation passed last year and enacted into law that we hope will help improve FOIA responsiveness.

But, of course, anything you can add to the FOIA consideration process is going to slow it down. That is one of the reasons why it is so critical that CUI not be yet another hurdle that FOIA requesters are going to have to get past in order to get their information.

Mr. REICHERT. Yeah. I had the same experience in the sheriff's office with public disclosure requests. They can slow down your entire organization. So I do have concern about that. Hopefully we can work together in lessening our fear of how that might affect FOIA requests.

I yield back. Thank you, Madam Chair.

Ms. HARMAN. Thank you, Mr. Reichert.

Mr. Carney of Pennsylvania is now recognized for 5 minutes.

Mr. CARNEY. Thank you, Madam Chair.

I would suggest also that one of the reasons we see overclassification sometimes is fear of embarrassment, political embarrassing things. In my experience at the Pentagon over a number of years, I did see some of that occur as well, and I think that is awful. You know, we have to get a handle on that, and we have to find ways to manage it.

But we are talking about DHS today. Is there some of that, actually, in this overclassification, do you think, hiding politically embarrassing things?

Ms. FUCHS. Well, I mean, I certainly think that there is some of that. I mean, a good example of that would be the Taguba report that first was looking at treatment of people in Abu Ghraib, which was largely classified. Obviously there may have been, you know, aspects of what happened that needed to be classified. There also may have been reasons to manage how the information was released. But, in fact, most of it did not require classification and eventually was released.

So I think there are numerous examples of the attempt to cover up embarrassing things that happened. But, of course, the reason we have these open-government laws is to expose those things so we can do better. That is why it is so important not to let that happen and why it is so important that this bill has provisions for looking at the decisions to label and then taking steps when it is improperly done.

Ms. MCDERMOTT. I agree with that, certainly, with overclassification. To the extent that we can tell, with the CUI markings, that is a very high risk, because there has been no control on them. There has been no control on who can create them. There has been no mechanism for removing them. At least with classified information, there are processes. So I think that is a very high risk, that they are for hiding embarrassing or inconvenient facts. So I think that is very important.

I would also like to note that, in terms of the FOIA—I know this wasn't your question—but if information is made proactively available by agencies that can be made available, it releases the need for FOIA.

Ms. FREDRICKSON. At the risk of repeating something that Meredith said earlier, I wouldn't necessarily classify it as embarrassing information, but the torture memos or the memos about interrogation methods that were prepared by the Office of Legal Counsel, you know, obviously, there, again, maybe sections of those that could have remained classified of what we haven't seen yet, but really this is information we need to know. The reason that it was classified was not because it was essentially a document that need-

ed to be withheld from the public, but really because I think that the legal analysis that was provided in those memos was so faulty.

Mr. CARNEY. From a DHS perspective, what do you see as the key DHS barriers to compliance with the Public Access to Documents Act?

Ms. FUCHS. I think the people I have dealt with at DHS seem like they have a genuinely strong intent to try to get better control over their information and to handle it properly. Although, I know that other agencies actually have a lot of problems with how DHS has handled information. So I think that, you know, DHS continues to struggle with the same problems that it has had, which are that it is a very large agency with lots of different missions and components. The CUI framework is going to require them to get some organization. I think Chair Harman mentioned, you know, bring order to the chaos, and I think that that is a big challenge at DHS and will continue to be so.

However, by reducing the number of controllers so you can focus on people who are going to put the labels on the information and by training them and supervising them properly, I think it will have a good impact.

Ms. MCDERMOTT. I agree with Ms. Fuchs that there are good people with good intent in the Department. But I was the one that said that they are the poster child of nontransparency, and they are. It is impossible to find information on their site. I have bookmarked regulatory information, submitted comments and gone back the next day, and they were gone, they were unfindable.

So I think it is going to be a serious challenge for the Department to implement this in a transparent and open manner. I think it is going to take continual oversight.

Again, I agree with Ms. Fuchs that there are good people with good intent, but the tendency of the Department is not toward transparency. Maybe with other agencies, but not with the public.

Ms. FREDRICKSON. Just quickly, I would just like to comment that the legislation that we are discussing today is actually not just an open-government bill but also a good-government bill, in the sense that I think there are real efficiencies in reducing the number of designations that are allowed. I think the cost savings that could result from Government actually being able to talk to other elements and getting the influence or advice of outside stakeholders is very critical to making it work better. So we support it on that basis, as well.

Mr. CARNEY. Thank you.

No further questions, ma'am.

Ms. HARMAN. Thank you.

I would just note for the record, as we discuss documents that supposedly explain the legal framework for Government programs, that, as a member of the Intelligence Committee all those years, we continually demanded to see those documents. They were never shown to us, at least during the time that I served on that committee.

On this committee, we have had an ongoing request to DHS about the legal underpinnings of the proposed National Applications Office, the NAO, which will task military satellites to do surveillance activities over the United States. We think that may pose

some problems under posse comitatus and some other issues. But, at any rate, that conversation is ongoing. We are not satisfied that we have seen a document explaining the legal underpinnings. That document should be available to Congress, which has responsibility for faithfully executing the laws, and the public should understand what the legal basis for government programs is, in my view.

I now yield 5 minutes for questions to Mr. Dent of Pennsylvania.

Mr. DENT. Thank you, Madam Chair.

From your viewpoint, is there "sensitive but unclassified" information out there that needs to be protected? Or do you believe that all unclassified information should be releasable without restriction by the Government, even if that information is sensitive? I would just be curious to get your thoughts on that.

Ms. MCDERMOTT. Oh, absolutely, there is controlled unclassified information that does need to be protected for at least a certain amount of time. I think the White House framework is intended to do that. I think that this bill takes important steps toward building in provisions to ensure that that is reviewed on a regular basis. The framework also includes portion marking, so that where there is a document, a portion of which needs to be kept safeguarded for a particular amount of time, that portion can be separated out and shared with those who need to have only that protected information, but the rest of the information can be shared more generally with the public.

So, absolutely, yes. But, as with classified information, most classified information also has a shelf life, except for sources and methods. There needs to be opportunities to review it and to remove the controls.

Mr. DENT. Ms. Fuchs.

Ms. FUCHS. I agree. I think that there is a need for some controls. I mean, to take it away from the specific information we are talking about, it is just like in any business, there is certain information you don't leave on your desk. Certainly CUI information, whether it is privacy information or it is information about a law enforcement investigation, it shouldn't be left around for, you know, the janitor to pick up. That is absolutely clear.

What I think we advocate for, though, is understanding what really needs that protection and not spending time and money on things that don't need that protection. That is why I think the CUI framework is necessary. But this bill fortunately would make sure the CUI framework does not become so broad that it pulls in too much information.

Mr. DENT. Thank you.

Ms. Fredrickson.

Ms. FREDRICKSON. I don't have too much to add to that. I entirely agree with the previous comments.

Just to say, I think it is important, as the Chair mentioned, that we need to move from a need-to-know to a need-to-share system, that the presumption has been too much on the side of nondisclosure. So where there are categories that are clearly—there is a heightened sensitivity, there needs to be a heightened sensitivity that we need to disclose as much as possible.

Mr. DENT. My next question, then, really deals with—the legislation that we are discussing today, H.R. 6193, applies only to the

Homeland Security Department. Do you think that a CUI framework should be established throughout the entire Federal Government? If so, what do you think is the best way to establish such a framework? What sorts of standards should be set in establishing that kind of a framework? Anyone want to take a shot at that?

Ms. FREDRICKSON. Sure. I think we spoke to that a little bit earlier. I think there is general agreement that it should be Government-wide. This bill provides, I think, a very good framework for expansion to other parts of the government.

Ms. MCDERMOTT. Well, I think we are all agreed that the current situation with what we previously called "sensitive but unclassified" information is untenable. It is untenable for the Government, it is untenable for the public, it is untenable for other governments who need to get information from the Government.

So a framework to deal with this is essential. The White House memorandum has established, sort of, the bare bones of that. We are pleased that the implementation has been put in the National Archives, which has a commitment to openness and would very much like to see most of the provisions of this bill adopted by NARA as it goes out to the information-sharing environment and then as other agencies adopt this framework.

Ms. FUCHS. I would just agree with what my other copanelists have said.

Mr. DENT. That is fine.

I yield back. Thank you.

Ms. HARMAN. Thank you, Mr. Dent.

Mr. Langevin is now recognized for 5 minutes for questions.

Mr. LANGEVIN. Thank you, Madam Chair.

I want to thank our witnesses for the testimony today.

I especially want to thank the Chair for holding this important meeting, this hearing today.

The Chair and I both have an appreciation for and love of intelligence work, and we can deeply appreciate views associated with a need for classified information. But equally important, we share an understanding that we need to get the information into the hands of those who need it and, equally important, giving the information to the public for their understanding of information as well.

Most of the questions that I had have really already been asked, but I do have a question with respect to how we proceed from here.

As we move forward with the implementation of the CUI designation, what are the most important things that Congress should be doing to ensure appropriate oversight? What do you see we need to do, in terms of overcoming the likely challenges with the implementation of CUI?

Ms. FREDRICKSON. That is a very good question, I think. That has obviously been a challenge for Congress for the past several years, oversight with this Government, particularly with its inclination toward secrecy, I think has really impeded a full and thorough oversight process. But I think the engagement of this committee and your commitment on the issue I think is clearly a very, very good step in the right direction.

Maintaining your attention on these issues, I think, will be required. I think, as Patrice had suggested, it will be a real task, I think, to push DHS forward and to ensure that the language of the

legislation is actually implemented in a way that is full and effective. So we are very eager to work with you. I also think it is also very important that the legislation does include the role of civil liberties and open-government organizations as well as the private sector to help ensure that the process moves forward effectively. I think, working together, perhaps we can really make that difference.

Ms. MCDERMOTT. I agree with Ms. Fredrickson.

I would also note that some of the provisions in this bill will be really important Government-wide. One of, I think, the most important ones for congressional oversight is the audits and the provision in the bill that also tracks the markings and uses by individual employees.

I think both of those—that should include a report to Congress also about specified individuals, but I think a reporting requirement to Congress and to the appropriate committees—yours for DHS and others as this goes out further—are essential to both the public trust in this and to Congress's ability to engage in oversight.

Then I also think the two other provisions, the ability for the public to ask for removal, because that gets us out in a more transparent realm, and the ability of employees to challenge the markings, is critical. Again, protection for employees that do that, because it is very nice to say they have the ability, but we know from experience that those challenges often lead to repercussions on the employees.

Ms. FUCHS. If I could just add a couple of other points. I think, it is very important for Congress to keep in mind the impact of this on the Freedom of Information Act and to not permit a memorandum that sets up the CUI framework to undermine the FOIA, which is a congressionally enacted statute.

I also think that Congress should be keeping an eye on the development of substantive definitions for CUI within each agency. This committee looks at the Department of Homeland Security, but every other committee should be looking at their own agencies that they conduct oversight over and make sure that the CUI definition does not become too expansive.

Finally, and this relates to what Ms. McDermott just said, I think it is important for Congress to keep an eye on how this is working, because, as I mentioned in my testimony, these trusted pathways could be corrupted just like an agency could be corrupted. In order for them to work, we need to make sure that those who are sharing the information understand that they are expected to use it properly and use those trusted pathways to help protect the country.

Mr. LANGEVIN. I appreciate all those answers. I think this legislation could be and should be a model Government-wide. I think Mr. Dent raised the question, should we—this applies to the Department of Homeland Security, but should it be Government-wide? I clearly think it should.

You know, classifying information runs the gamut. I think we have all been frustrated by this overclassification in a number of areas. You know, it seems to run the gamut from doing it out of an abundance of caution, to maybe protecting politically sensitive or embarrassing information, to just pure laziness.

We have all been frustrated, those of us who see classified information, a lot of times you look at it and say, and we have asked often, is there really a need to classify this? What is classified about this information? I think it does come down sometimes to just pure laziness. So we need someone that is going to actually ask the question, why do we really need to classify this information?

So I think this legislation moves us in the right direction so that we can ensure that the public has access to information it needs, that we get information that may be sensitive into the hands of those who need to see it so we are ensuring proper information-sharing, and that we are only classifying those things that really do need to be classified.

So I commend the Chair for the legislation and for the hearing. With that, I will yield back. Thank you.

Ms. HARMAN. Thank you, Mr. Langevin.

I have asked the Members to my right whether they have additional questions. They don't.

Do you have any additional questions?

Well, okay. Then let me just make a couple of comments, and we will adjourn, followed by the markup that has been announced, in 15 minutes after adjournment, of the four bills. My comments are as follows.

First, thank you to our witnesses and to other outside groups and administration experts for contributing to our work on this piece of legislation. I think it is a much better piece of legislation because we consulted widely and because we worked together. Mr. Reichert and his staff were enormously helpful in improving the legislation.

Second, we are building on a Bush administration framework. I am saying this; it is true. Ambassador McNamara is the fellow who came out with the CUI guidelines. He was tasked to do this. We are trying to find a way to make DHS, the Department of Homeland Security, the gold standard for implementing those guidelines correctly. So here we have a committee of Congress building on Bush administration guidelines. It will be a rare, I think final, example of such a thing. But I think we are going to build something important because of the way we worked on this.

Finally, one of you was talking about the need to involve the public in advance—I think this is what you said, or this is certainly what I wanted you to say because I agree with it—in advance in understanding the terror threats we face. Let's understand what the motivation of terrorists is. They want to terrify us. Some of them may also want to kill as many of us as possible. But that is the point of their activity, is to terrify us.

I believe that an informed and prepared public is much less likely to be terrified. How do we inform the public? Well, part of it is sharing information with the public, having a presumption that unless there is a good reason not to share it, it must be shared. Second, having public officials who, in a thoughtful and useful way, brief the public on what the threats are and what to do to protect themselves—not terrify them, not scare them; brief them, inform them. An informed public, I think, is our best protection of democracy. It is also our best protection against terrorism.

So I want to say that, by doing this legislation and by enacting the other bills on public access that we will enact, I believe we will enact today on a unanimous basis, I think we are taking a giant step toward one of the big missions of this committee, which is protecting the homeland.

I want to thank you all for your contribution to this.

I also want to say that if any Members have additional questions for the witnesses, we will ask you to respond expeditiously in writing to those questions.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 11:12 a.m., the subcommittee was adjourned.]