AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

110TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
110–779

IMPROVING PUBLIC ACCESS TO DOCUMENTS ACT OF 2008

JULY 28, 2008.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 6193]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 6193) to require the Secretary of Homeland Security to develop and administer policies, procedures, and programs to promote the implementation of the Controlled Unclassified Information Framework applicable to unclassified information that is homeland security information, terrorism information, weapons of mass destruction information and other information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	6
Background and Need for Legislation	6
Hearings	8
Committee Consideration	9
Committee Votes	9
Committee Oversight Findings	9
New Budget Authority, Entitlement Authority, and Tax Expenditures	9
Congressional Budget Office Estimate	10
Statement of General Performance Goals and Objectives	11
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	11
Federal Mandates Statement	12
Advisory Committee Statement	12
Constitutional Authority Statement	12

69–006

Applicability to Legislative Branch 12
Section-by-Section Analysis of the Legislation 12
Changes in Existing Law Made by the Bill, as Reported 14
Committee Correspondence 21

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Improving Public Access to Documents Act of 2008".

SEC. 2. FINDINGS.

Congress finds the following:

(1) The proliferation and widespread use of "sensitive but unclassified" (SBU) control markings by the Federal Government interferes with accurate, actionable, and timely homeland security information sharing, increases the cost of information security, and needlessly limits public access to information.

(2) The control markings problem, which has worsened since the 9/11 attacks, causes considerable confusion about what information can be shared with whom both internally at the Department of Homeland Security and with its external partners. This problem negatively impacts the dissemination of homeland security information to the Department's State, local, tribal, and territorial homeland security and law enforcement partners, private sector customers, and the public.

(3) Overuse of "sensitive but unclassified" markings stands in the way of a safer and more secure homeland. This trend is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), and must be halted and reversed.

(4) To do so, the Department should start with the understanding that all departmental information that is not properly classified, or marked as controlled unclassified information and otherwise exempt from disclosure, should be made available to members of the public pursuant to section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act").

(5) The Department should also develop and administer policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of controlled unclassified information markings and the National Archives and Records Administration policies implementing them.

SEC. 3. CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION WITHIN THE DEPARTMENT OF HOMELAND SECURITY.

Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 210F. CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION PROGRAM.

"(a) IN GENERAL.—The Secretary shall develop and administer policies, procedures, and programs within the Department to implement the controlled unclassified information framework to standardize the use of controlled unclassified markings on, and to maximize the disclosure to the public of, homeland security information, terrorism information, weapons of mass destruction information, and other information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) that must be disseminated to prevent and to collectively respond to acts of terrorism. The Secretary shall coordinate with the Archivist of the United States and consult with representatives of State, local, tribal, and territorial government and law enforcement, organizations with expertise in civil rights, civil liberties, and government oversight, and the private sector, as appropriate, to develop such policies, procedures, and programs.

"(b) REQUIREMENTS.—Not later than one year after the date of the enactment of the Improving Public Access to Documents Act of 2008, the Secretary, in administering the policies, procedures, and programs required under subsection (a), shall—

"(1) create, in consultation with the Archivist of the United States, a standard format for unclassified finished intelligence products created by the Department that have been designated as controlled unclassified information, consistent with any government-wide standards, practices or procedures for similar products;

"(2) require that all unclassified finished intelligence products created by the Department that have been designated as controlled unclassified information be prepared in the standard format;

"(3) ensure that such policies, procedures, and programs protect the national security as well as the information privacy rights and legal rights of United States persons pursuant to all applicable law and policy, including the privacy guidelines for the information sharing environment established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), as appropriate;

"(4) establish an ongoing auditing mechanism administered by the Inspector General of the Department or other appropriate senior Department official that randomly selects, on a periodic basis, controlled unclassified information from each component of the Department, including all Department components that generate unclassified finished intelligence products, to—

"(A) assess, on an individualized basis, whether applicable controlled unclassified information policies, procedures, rules, and regulations have been followed;

"(B) describe any problems with the administration of the applicable controlled unclassified information policies, procedures, rules and regulations, including specific non-compliance issues;

"(C) recommend improvements in awareness and training to address them; and

"(D) report at least annually to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, and the public on the findings of the Inspector General's audits under this section;

"(5) establish a process whereby employees may challenge the use of controlled unclassified information markings by Department employees or contractors and be rewarded with specific incentives for successful challenges resulting in—

"(A) the removal of controlled unclassified information markings; or

"(B) the correct application of appropriate controlled unclassified information markings;

"(6) inform employees and contractors that failure to comply with the policies, procedures, and programs established under this section could subject them to a series of penalties;

"(7) institute a series of penalties for employees and contractors who repeatedly fail to comply with the policies, procedures, and programs established under this section after having received both notice of their noncompliance and appropriate training or re-training to address such noncompliance;

"(8) maintain a publicly available list of all documents designated, in whole or in part, as controlled unclassified information by Department employees or contractors that—

"(A) 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

"(B) includes for each such withheld document a summary of the request and a statement that identifies the exemption under section 552(b) of title 5, United States Code (commonly referred to as the 'Freedom of Information Act') that justified the withholding; and

"(9) create a process through which the public can notify the Inspector General of the Department of any concerns regarding the implementation of the controlled unclassified information framework, including the withholding of controlled unclassified information pursuant to section 552(b) of title 5, United States Code (commonly referred to as the 'Freedom of Information Act'), which shall be considered as part of the audit described in paragraph (4).

"(c) IMPLEMENTATION.—In carrying out subsections (a) and (b), the Secretary shall ensure that—

"(1) information is designated as controlled unclassified information and includes an authorized controlled unclassified information marking only if—

"(A) a statute or executive order requires or authorizes such a designation and marking; or

"(B) the Secretary, through regulations, directives, or other specific guidance to the agency that have been submitted to and approved by the Archivist of the United States, determines that the information is controlled unclassified information based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, safety, or security;

"(2) notwithstanding paragraph (1), information is not to be designated as controlled unclassified information—

"(A) to conceal violations of law, inefficiency, or administrative error;

"(B) to prevent embarrassment to Federal, State, local, tribal, or territorial governments or any official, agency, or organization thereof; any agency; or any organization;

"(C) to improperly or unlawfully interfere with competition in the private sector;

"(D) to prevent or delay the release of information that does not require such protection;

"(E) if it is required to be made available to the public; or

"(F) if it has already been released to the public under proper authority; and

"(3) the controlled unclassified information framework is administered in a manner that ensures that—

"(A) information can be shared within the Department and with State, local, tribal, and territorial governments, the private sector, and the public, as appropriate;

"(B) all policies and standards for the designation, marking, safeguarding, and dissemination of controlled unclassified information are consistent with the controlled unclassified information framework and any other policies, guidelines, procedures, instructions, or standards established by the President, including in any relevant future executive memoranda or executive orders;

"(C) the number of Department employees and contractors with controlled unclassified information designation authority is limited appropriately as determined in consultation with the parties referred to in subsection (a);

"(D) controlled unclassified information markings are not a determinant of public disclosure pursuant to section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act');

"(E) controlled unclassified information markings are placed on archived or legacy material whenever circulated, consistent with the controlled unclassified information framework and any other policies, guidelines, procedures, instructions, or standards established by the President, including in any relevant future executive memoranda or executive orders;

"(F) all controlled unclassified information portions of classified documents are marked as controlled unclassified information; and

"(G) it supersedes any pre-existing policies and procedures relating to the creation, control, and sharing of sensitive but unclassified information generated by the Department, except where otherwise provided by law.

"(d) PUBLIC ACCESS TO UNCLASSIFIED INFORMATION.—The Secretary shall make available to members of the public all controlled unclassified information and other unclassified information in its possession that is releasable pursuant to an appropriate request under section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act').

"(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prevent or discourage the Department from voluntarily releasing to the public any unclassified information that is not exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act').".

SEC. 4. ENFORCEMENT OF CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION WITHIN THE DEPARTMENT OF HOMELAND SECURITY.

Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 210G. ENFORCEMENT OF CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION PROGRAMS.

"(a) PERSONAL IDENTIFIERS.—The Secretary shall—

"(1) assess the technologies available or in use at the Department by which an electronic personal identification number or other electronic identifying marker can be assigned to each Department employee and contractor with controlled unclassified information designation authority in order to—

"(A) track which documents have been designated as controlled unclassified information by a particular employee or contractor;

"(B) determine the circumstances when such documents have been shared;

"(C) identify and address misuse of controlled unclassified information markings, including the misapplication of controlled unclassified information markings to documents that do not merit such markings; and

"(D) assess the information sharing impact of any such problems or misuse;

"(2) develop an implementation plan for a Department standard for such technology with appropriate benchmarks, a timetable for its completion, and cost estimate for the creation and implementation of a system of electronic personal identification numbers or other electronic identifying markers for all relevant Department employees and contractors; and

"(3) upon completion of the implementation plan described in paragraph (2), or not later than 180 days after the date of the enactment of the Improving Public Access to Documents Act of 2008, whichever is earlier, the Secretary shall provide a copy of the plan to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

"(b) TRAINING.—The Secretary, in coordination with the Archivist of the United States, shall—

"(1) require annual training for each Department employee and contractor with controlled unclassified information designation authority and who are responsible for analysis, dissemination, preparation, production, receiving, publishing, or otherwise communicating written controlled unclassified information. Such training shall—

"(A) educate each employee and contractor about—

"(i) the Department's requirement that all unclassified finished intelligence products that they create that have been designated as controlled unclassified information be prepared in a standard format prescribed by the Department;

"(ii) the proper use of controlled unclassified information markings, including portion markings; and

"(iii) the consequences of improperly using controlled unclassified information markings, including the misapplication of controlled unclassified information markings to documents that do not merit such markings, and of failing to comply with the Department's policies and procedures established under or pursuant to this section, including the negative consequences for the individual's personnel evaluation, homeland security, information sharing, and the overall success of the Department's missions;

"(B) serve as a prerequisite, once completed successfully, as evidenced by an appropriate certificate, for—

"(i) obtaining controlled unclassified information designation authority; and

"(ii) renewing such authority annually; and

"(C) count as a positive factor, once completed successfully, in the Department's employment, evaluation, and promotion decisions; and

"(2) ensure that such program is conducted efficiently, in conjunction with any other security, intelligence, or other training programs required by the Department to reduce the costs and administrative burdens associated with the additional training required by this section.

"(c) DETAILEE PROGRAM.—The Secretary shall—

"(1) implement a Departmental detailee program to detail Departmental personnel to the National Archives and Records Administration for one year, for the purpose of—

"(A) training and educational benefit for the Department personnel assigned so that they may better understand the policies, procedures, and laws governing the controlled unclassified information framework;

"(B) bolstering the ability of the National Archives and Records Administration to conduct its oversight authorities over the Department and other Departments and agencies; and

"(C) ensuring that the policies and procedures established by the Secretary remain consistent with those established by the Archivist of the United States; and

"(2) in coordination with the Archivist of the United States, report to Congress not later than 90 days after the conclusion of the first year of the program established under paragraph (1), on—

"(A) the advisability of expanding the program on a government-wide basis, whereby other departments and agencies would send detailees to the National Archives and Records Administration; and

"(B) the administrative and monetary costs of full compliance with this section.

"(d) TERMINATION OF DETAILEE PROGRAM.—Except as otherwise provided by law, subsection (c) shall cease to have effect on December 31, 2012.".

SEC. 5. DEFINITIONS.

Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following new section:

"SEC. 210H. DEFINITIONS.

"In this Act:

"(1) CONTROLLED UNCLASSIFIED INFORMATION.—The term 'controlled unclassified information' means a categorical designation that refers to unclassified information, including unclassified information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including unclassified homeland security information, terrorism information, and weapons of mass destruction information (as defined in such section) and unclassified national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))), that does not meet the standards of National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or National Archives and Records Administration policy requires safeguarding from unauthorized disclosure, special handling safeguards, or prescribed limits on exchanges or dissemination.

"(2) CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK.—The term 'controlled unclassified information framework' means the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of terrorism-related controlled unclassified information that originates in departments and agencies, regardless of the medium used for the display, storage, or transmittal of such information, as set forth in the President's May 7, 2008 Memorandum for the Heads of Executive Departments Regarding Designation and Sharing of controlled unclassified information (CUI), and in any relevant future executive memoranda, executive orders, or legislation.

"(3) FINISHED INTELLIGENCE PRODUCT.—The term 'finished intelligence product' means a document in which an intelligence analyst has evaluated, interpreted, integrated, or placed into context raw intelligence or information.".

SEC. 6. TECHNICAL AMENDMENT.

The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101(b)) is amended by adding after the item relating to section 210E the following new items:

"Sec. 210F. Controlled unclassified information framework implementation program.
"Sec. 210G. Enforcement of controlled unclassified information framework implementation programs.
"Sec. 210H. Definitions.".

PURPOSE AND SUMMARY

The purpose of H.R. 6193 is to require the Secretary of Homeland Security to develop and administer policies, procedures, and programs to promote the implementation of the Controlled Unclassified Information Framework applicable to unclassified information that is homeland security information, terrorism information, weapons of mass destruction information and other information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

The Final Report of the National Commission on Terrorist Attacks Upon the United States, commonly known as the "9/11 Commission Report", found that the Federal Intelligence Community's information security policies and practices impeded the kinds of robust information sharing required to prevent and otherwise prepare for terrorist attacks. Specifically, it found that security requirements nurtured over-classification and excessive compartmentation of information among agencies in several respects: (1) each agency's incentive structure opposed sharing, with

clear risks but few rewards for sharing information; (2) no one had to pay the long term costs of over-classifying information, though this cost is substantial; (3) there were no punishments for not sharing information; and (4) agencies upheld a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.

The global nature of the threats that the homeland faces today makes it vital that the Nation's entire network of defenders be able to share information more rapidly and confidently so that those who must act have the information they need. The excessive compartmentation of information described in the 9/11 Commission Report involves the proliferation and overuse of sensitive but unclassified (SBU) control markings—such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Sensitive Homeland Security Information (SHSI)—to protect unclassified homeland security and other information. Although these documents do not include classified material, their authors believe that they nevertheless have the potential to compromise the Nation's security if they become public. While it is important that the Government protect truly sensitive unclassified information, including protecting the privacy and other legal rights of Americans, the lack of a uniform Government-wide framework for handling SBU information impedes both information sharing and the intended protective function of SBU information control markings. Further, recipients of SBU information often do not have proper guidance on how to handle it.

SBU information traditionally has been shared according to an ungoverned body of policies and practices that confuse both its producers and users. At least 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information exist across the Federal Government. These processes and procedures fall into three general categories: (1) those that were created by statute or implement a statute; (2) those that were created by a Federal regulation based on a notice-and-comment rulemaking process; and (3) those that are based on individual agency and department directives, orders, or other administrative documents. The majority of them have been derived from documents that address specific agency or department missions—resulting in considerable inconsistency across Federal agencies and departments. This is particularly problematic when it comes to homeland security. According to the Government Accountability Office, Federal agencies that account for a large percentage of the homeland security budget reported using the most SBU information control markings.

These markings are having a negative impact on the sharing of accurate, actionable, and timely homeland security and other information with the people who need it. Unlike classified records or ordinary agency records, there is neither monitoring of nor reporting on the use or impact of SBU information control markings nor is there a procedure for the public to challenge the use of such markings. The Committee believes that given the wide variation in control marking practices and procedures, as well as some of their features, SBU information control markings needlessly interfere with interagency information sharing, increase the cost of information security, and limit public access to vital information. The Com-

mittee further believes that the current SBU information regime has in many respects deterred information sharing for homeland security purposes—becoming, in effect, a de facto classification system in its own right.

A Government-wide SBU information framework that is rational, standardized, and simplified will facilitate the creation of an Information Sharing Environment that not only supports the individual missions of agencies and departments but also enhances their ability to share vital terrorism information with key stakeholders. The President, through the Program Manager of the Information Sharing Environment, released a new Controlled Unclassified Information (CUI) Framework in May 2008 for this purpose. If implemented correctly at the Department and across the Federal Government, the framework will satisfy the dual imperatives of improving information sharing while protecting SBU information (now known as "CUI") under appropriate circumstances. This measure therefore requires the Department to implement the CUI Framework with all deliberate speed. The potential dividends for more and better information sharing—and homeland security—are enormous.

HEARINGS

On March 22, 2007, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment held a hearing entitled "Over-classification and Pseudo-classification: The Impact on Information Sharing." The Subcommittee received testimony from Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration, Mr. Scott Armstrong, Founder, Information Trust, Ms. Meredith Fuchs, General Counsel, The National Security Archive, George Washington University, Chief Cathy L. Lanier, Metropolitan Police Department, Washington, D.C., and Mr. Michael P. Downing, Assistant Commanding Officer, Counter—Terrorism/Criminal Intelligence Bureau, Los Angeles Police Department.

On April 26, 2007, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment held a hearing entitled "The Over-Classification and Pseudo-Classification of Government Information: The Response of the Program Manager of the Information Sharing Environment." The Subcommittee received testimony from Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence; Carter Morris, Ph.D., Director, Informational Sharing and Knowledge Management, Office of Intelligence and Analysis, Department of Homeland Security; Mr. Wayne M. Murphy, Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation, Department of Justice, Colonel Bart R. Johnson, New York State Police; and Mr. Mark Zadra, Assistant Commissioner, Florida Department of Law Enforcement.

On June 28, 2007, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment held a hearing entitled "Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information." The Subcommittee received testimony from Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Record Administration; Mr. Scott

Armstrong, Founder, Information Trust; Ms. Suzanne E. Spaulding, Principal, Bingham Consulting Group, LLC; and Mr. Mark Agrast, Senior Fellow, Center for American Progress.

On June 11, 2008, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment held a hearing on H.R. 6193. The Subcommittee received testimony from Ms. Meredith Fuchs, General Counsel, National Security Archive; Ms. Caroline Fredrickson, Director, Washington Legislative Office, American Civil Liberties Union; and Ms. Patrice McDermott, Director, OpenTheGovernment.org.

COMMITTEE CONSIDERATION

H.R. 6193 was introduced in the House on June 5, 2008, by Ms. Harman, and seven original co-sponsors and referred solely to the Committee on Homeland Security. Within the Committee H.R. 6193 was referred to the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

The Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment considered H.R. 6193 on June 11, 2008, and ordered the measure favorably forwarded to the Full Committee for consideration, amended, by unanimous consent.

The following amendment was offered:

> An Amendment in the Nature of a Substitute offered by Ms. Harman (#1), was AGREED TO by unanimous consent.

On June 26, 2008, the Committee on Homeland Security considered H.R. 6193 and ordered the measure to be reported to the House favorably, as amended, by voice vote.

The following amendment was offered:

> An Amendment in the Nature of a Substitute offered by Ms. Harman (#1); was AGREED TO by unanimous consent.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes occured during consideration.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 6193, the Improving Public Access to Documents Act of 2008, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE
Washington, DC, July 10, 2008.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 6193, the Improving Public Access to Documents Act of 2008.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

ROBERT A. SUNSHINE
(For Peter R. Orszag, Director).

Enclosure.

H.R. 6193—Improving Public Access to Documents Act of 2008

H.R. 6193 would make several amendments to the Homeland Security Act of 2002 designed to promote the sharing of homeland security and intelligence information by the Department of Homeland Security (DHS). In particular, the bill would direct the Secretary of DHS to develop, in consultation with the National Archives and Records Administration, a standard format for intelligence products that are designated as controlled unclassified information (CUI), and directs DHS to share, when appropriate, such information with state and local governments, the private sector, and the public. The bill also would require periodic auditing of information designated as CUI and annual training for DHS employees on the proper format for such products.

In addition, the bill would require DHS to assess technologies that would allow the department to track the designation and sharing of CUI, and to develop a plan for implementing such technologies. Since the bill would not require DHS to deploy such technologies, this estimate does not include implementation costs. However, based on information from DHS and the Office of the Director of National Intelligence, CBO anticipates that such costs could be significant.

DHS would incur small incremental costs related primarily to the periodic auditing of CUI and the additional training that would be required by the bill. Since DHS is required to monitor compliance with existing policies and has an annual training program for its employees, CBO estimates that the cost of implementing H.R. 6193 would be less than $500,000 a year, assuming the availability of appropriated funds. Enacting the legislation would not affect direct spending or revenues.

H.R. 6193 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is Jason Wheelock. This estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 6193 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

The Controlled Unclassified Information (CUI) Framework, which reduces the number of such allowable SBU markings from over 107 to just seven, appears to be a workable replacement for the out-of-control SBU information practices, policies, and procedures that have plagued the Federal Government for too long. This measure requires the Department of Homeland Security to adopt a CUI Framework Implementation Plan with rigorous policy development, training, and auditing requirements that will promote accountability and best practices as the Department operationalizes the new control marking regime. In so doing, it will make the Department the "gold standard" when it comes to getting the CUI Framework up and running—and working—correctly. Although a Government-wide implementation approach would be beneficial, the Department is an excellent place to start this important transition. H.R. 6193 will make the Department a center of excellence when it comes to using CUI control markings and a test bed for the rest of the Federal Government.

The goal of this measure is to ensure that Department employees and contractors apply the new CUI Framework in strict accordance with applicable law, executive orders, and other authorities in order to (1) standardize the use of CUI control markings on unclassified homeland security and other information within the scope of the Information Sharing Environment that must be disseminated to prevent and to collectively respond to acts of terrorism; and (2) maximize the disclosure of this information to the Department's State, local, and tribal partners and, as appropriate, to the public. To facilitate this change, this measure will accomplish several key objectives: (1) promote a common understanding among Department employees and contractors that CUI control markings are not to be used to protect political turf or to hide embarrassing facts from public view; (2) develop best practices that ensure that the Department's use of CUI control markings adheres to applicable laws, executive orders, and other relevant authorities; (3) promote a variety of accountability measures that identify CUI control marking problems and their sources and recommend and implement strategies to address them; and (4) bolster public confidence in the Department's homeland security and information sharing missions through these and other measures that promote accountability, integrity, and transparency across its intelligence enterprise.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional ear-

marks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common Defense of the United States.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that this measure may be cited as the "Improving Public Access to Documents Act of 2008".

Section 2. Findings

This section outlines a series of Congressional findings, including: (1) the proliferation and widespread use of "sensitive but unclassified" (SBU) control markings interferes with information sharing; increases the cost of information security; and needlessly limits public access to information; (2) this trend stands in the way of a safer homeland and must be halted and reversed; (3) accordingly, the Department of Homeland Security should start with the understanding that information that is not properly classified—or otherwise exempt from disclosure—should be made publicly available pursuant to an appropriate Freedom of Information Act (FOIA) request; and (4) the Department should develop and administer policies, procedures and programs that ensure that the newly released Controlled Unclassified Information (CUI) Framework, which is intended to supplant the use of SBU information control markings, is properly implemented.

Section 3. Controlled Unclassified Information Framework implementation program

This section modifies Title II of the Homeland Security Act of 2002 (P.L. 107–296) to require the Secretary of Homeland Security to coordinate the development and administration of policies, procedures and programs for the implementation of the Controlled Un-

classified Information (CUI) Framework at the Department of Homeland Security with the Archivist of the United States and to consult with organizations with expertise in civil rights, civil liberties, and governmental oversight.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary, in administering the policies, procedures, and programs required under this section, to (1) create a standard unclassified format for Finished Intelligence Products that have been designated as CUI; (2) require the use of that standard format; (3) ensure that not only the national security but also the privacy and other legal rights of United States persons are protected as part of the enforcement of the aforementioned policies, procedures, and programs; (4) establish, within one year of enactment, an ongoing auditing mechanism to ensure that, among other things, CUI policies, procedures, rules and regulations are being followed by Department employees and contractors; and (5) report to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the public on the findings of the Department's Inspector General about whether these requirements are being met, identifying any problems in this regard, and recommending improvements to address them.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary to establish a process to reward Department personnel for successful challenges to the use of CUI markings that result in the removal or appropriate usage of such markings. This section further requires the Secretary to institute a series of penalties for Department personnel who repeatedly fail to comply with applicable CUI policies, procedures, rules, and regulations after notice of their non-compliance and training or retraining to address such noncompliance.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary to maintain a publicly available list of documents that have been designated and marked, in whole or in part, as CUI and which have been withheld in response to a FOIA request. This section further requires the Secretary to create a process through which the public may notify the Inspector General of the Department of any concerns regarding the implementation of the CUI Framework, including the withholding of CUI pursuant to FOIA exemptions.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary to make available to the public, pursuant to an appropriate request under FOIA, all CUI and other unclassified information in its possession. It also clarifies that nothing in this measure shall be construed to prevent or discourage the Department from voluntarily making unclassified information available to the public.

Section 4. Enforcement of Controlled Unclassified Information Framework implementation within the Department of Homeland Security

This section modifies Title II of the Homeland Security Act of 2002 (P.L. 107–296) to require the Secretary of Homeland Security to assess technologies available or already in use at the Department of Homeland Security by which an electronic personal identi-

fication number or other electronic identifying marker can be assigned to each Department employee or contractor with Controlled Unclassified Information (CUI) designation authority in order to track which documents have been designated as CUI by a particular employee; identify and address misuse of CUI markings; and assess the information sharing impact of such misuse. This section requires the Secretary to develop an implementation plan for such technology at the Department and establishes a deadline for it.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary to develop a training program for the proper use of the CUI Framework for all employees and contractors who have CUI designation authority and who are responsible for analysis, dissemination, preparation, producing, receiving, publishing, or otherwise communicating written CUI. Among other things, it requires the training to address proper formats for finished intelligence products that are also CUI and the consequences of improper use of CUI markings. This section clarifies that such training serves as a prerequisite for obtaining CUI designation authority and renewing such authority annually. This section further requires the Secretary to coordinate with the Archivist of the United States in developing this training program.

This section further modifies Title II of the Homeland Security Act of 2002 to require the Secretary to establish a detailee program with the United States National Archives and Records Administration (NARA) that will train Department personnel about the policies, procedures, and laws governing the CUI Framework; bolster NARA's ability to conduct oversight over the Department; and ensure that Department policies are consistent with those established by the Archivist of the United States.

Section 5. Definitions

This section defines terms used in this measure.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

* * * * * * *

Sec. 210F. Controlled unclassified information framework implementation program.

Sec. 210G. Enforcement of controlled unclassified information framework implementation programs.
Sec. 210H. Definitions.

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

* * * * * * *

SEC. 210F. CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION PROGRAM.

(a) IN GENERAL.—The Secretary shall develop and administer policies, procedures, and programs within the Department to implement the controlled unclassified information framework to standardize the use of controlled unclassified markings on, and to maximize the disclosure to the public of, homeland security information, terrorism information, weapons of mass destruction information, and other information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) that must be disseminated to prevent and to collectively respond to acts of terrorism. The Secretary shall coordinate with the Archivist of the United States and consult with representatives of State, local, tribal, and territorial government and law enforcement, organizations with expertise in civil rights, civil liberties, and government oversight, and the private sector, as appropriate, to develop such policies, procedures, and programs.

(b) REQUIREMENTS.—Not later than one year after the date of the enactment of the Improving Public Access to Documents Act of 2008, the Secretary, in administering the policies, procedures, and programs required under subsection (a), shall—

(1) create, in consultation with the Archivist of the United States, a standard format for unclassified finished intelligence products created by the Department that have been designated as controlled unclassified information, consistent with any government-wide standards, practices or procedures for similar products;

(2) require that all unclassified finished intelligence products created by the Department that have been designated as controlled unclassified information be prepared in the standard format;

(3) ensure that such policies, procedures, and programs protect the national security as well as the information privacy rights and legal rights of United States persons pursuant to all applicable law and policy, including the privacy guidelines for the information sharing environment established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), as appropriate;

(4) establish an ongoing auditing mechanism administered by the Inspector General of the Department or other appropriate senior Department official that randomly selects, on a periodic basis, controlled unclassified information from each component of the Department, including all Department components that generate unclassified finished intelligence products, to—

(A) assess, on an individualized basis, whether applicable controlled unclassified information policies, procedures, rules, and regulations have been followed;

(B) describe any problems with the administration of the applicable controlled unclassified information policies, procedures, rules and regulations, including specific non-compliance issues;

(C) recommend improvements in awareness and training to address them; and

(D) report at least annually to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, and the public on the findings of the Inspector General's audits under this section;

(5) establish a process whereby employees may challenge the use of controlled unclassified information markings by Department employees or contractors and be rewarded with specific incentives for successful challenges resulting in—

(A) the removal of controlled unclassified information markings; or

(B) the correct application of appropriate controlled unclassified information markings;

(6) inform employees and contractors that failure to comply with the policies, procedures, and programs established under this section could subject them to a series of penalties;

(7) institute a series of penalties for employees and contractors who repeatedly fail to comply with the policies, procedures, and programs established under this section after having received both notice of their noncompliance and appropriate training or re-training to address such noncompliance;

(8) maintain a publicly available list of all documents designated, in whole or in part, as controlled unclassified information by Department employees or contractors that—

(A) 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

(B) includes for each such withheld document a summary of the request and a statement that identifies the exemption under section 552(b) of title 5, United States Code (commonly referred to as the "Freedom of Information Act") that justified the withholding; and

(9) create a process through which the public can notify the Inspector General of the Department of any concerns regarding the implementation of the controlled unclassified information framework, including the withholding of controlled unclassified information pursuant to section 552(b) of title 5, United States Code (commonly referred to as the "Freedom of Information Act"), which shall be considered as part of the audit described in paragraph (4).

(c) IMPLEMENTATION.—In carrying out subsections (a) and (b), the Secretary shall ensure that—

(1) information is designated as controlled unclassified information and includes an authorized controlled unclassified information marking only if—

(A) a statute or executive order requires or authorizes such a designation and marking; or

(B) the Secretary, through regulations, directives, or other specific guidance to the agency that have been submitted to and approved by the Archivist of the United States, determines that the information is controlled unclassified information based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, safety, or security;

(2) notwithstanding paragraph (1), information is not to be designated as controlled unclassified information—

(A) to conceal violations of law, inefficiency, or administrative error;

(B) to prevent embarrassment to Federal, State, local, tribal, or territorial governments or any official, agency, or organization thereof; any agency; or any organization;

(C) to improperly or unlawfully interfere with competition in the private sector;

(D) to prevent or delay the release of information that does not require such protection;

(E) if it is required to be made available to the public; or

(F) if it has already been released to the public under proper authority; and

(3) the controlled unclassified information framework is administered in a manner that ensures that—

(A) information can be shared within the Department and with State, local, tribal, and territorial governments, the private sector, and the public, as appropriate;

(B) all policies and standards for the designation, marking, safeguarding, and dissemination of controlled unclassified information are consistent with the controlled unclassified information framework and any other policies, guidelines, procedures, instructions, or standards established by the President, including in any relevant future executive memoranda or executive orders;

(C) the number of Department employees and contractors with controlled unclassified information designation authority is limited appropriately as determined in consultation with the parties referred to in subsection (a);

(D) controlled unclassified information markings are not a determinant of public disclosure pursuant to section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act");

(E) controlled unclassified information markings are placed on archived or legacy material whenever circulated, consistent with the controlled unclassified information framework and any other policies, guidelines, procedures, instructions, or standards established by the President, in-

cluding in any relevant future executive memoranda or executive orders;

(F) all controlled unclassified information portions of classified documents are marked as controlled unclassified information; and

(G) it supersedes any pre-existing policies and procedures relating to the creation, control, and sharing of sensitive but unclassified information generated by the Department, except where otherwise provided by law.

(d) PUBLIC ACCESS TO UNCLASSIFIED INFORMATION.—The Secretary shall make available to members of the public all controlled unclassified information and other unclassified information in its possession that is releasable pursuant to an appropriate request under section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act").

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prevent or discourage the Department from voluntarily releasing to the public any unclassified information that is not exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act").

SEC. 210G. ENFORCEMENT OF CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK IMPLEMENTATION PROGRAMS.

(a) PERSONAL IDENTIFIERS.—The Secretary shall—

(1) assess the technologies available or in use at the Department by which an electronic personal identification number or other electronic identifying marker can be assigned to each Department employee and contractor with controlled unclassified information designation authority in order to—

(A) track which documents have been designated as controlled unclassified information by a particular employee or contractor;

(B) determine the circumstances when such documents have been shared;

(C) identify and address misuse of controlled unclassified information markings, including the misapplication of controlled unclassified information markings to documents that do not merit such markings; and

(D) assess the information sharing impact of any such problems or misuse;

(2) develop an implementation plan for a Department standard for such technology with appropriate benchmarks, a timetable for its completion, and cost estimate for the creation and implementation of a system of electronic personal identification numbers or other electronic identifying markers for all relevant Department employees and contractors; and

(3) upon completion of the implementation plan described in paragraph (2), or not later than 180 days after the date of the enactment of the Improving Public Access to Documents Act of 2008, whichever is earlier, the Secretary shall provide a copy of the plan to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(b) TRAINING.—The Secretary, in coordination with the Archivist of the United States, shall—

(1) require annual training for each Department employee and contractor with controlled unclassified information designation authority and who are responsible for analysis, dissemination, preparation, production, receiving, publishing, or otherwise communicating written controlled unclassified information. Such training shall—

(A) educate each employee and contractor about—

(i) the Department's requirement that all unclassified finished intelligence products that they create that have been designated as controlled unclassified information be prepared in a standard format prescribed by the Department;

(ii) the proper use of controlled unclassified information markings, including portion markings; and

(iii) the consequences of improperly using controlled unclassified information markings, including the misapplication of controlled unclassified information markings to documents that do not merit such markings, and of failing to comply with the Department's policies and procedures established under or pursuant to this section, including the negative consequences for the individual's personnel evaluation, homeland security, information sharing, and the overall success of the Department's missions;

(B) serve as a prerequisite, once completed successfully, as evidenced by an appropriate certificate, for—

(i) obtaining controlled unclassified information designation authority; and

(ii) renewing such authority annually; and

(C) count as a positive factor, once completed successfully, in the Department's employment, evaluation, and promotion decisions; and

(2) ensure that such program is conducted efficiently, in conjunction with any other security, intelligence, or other training programs required by the Department to reduce the costs and administrative burdens associated with the additional training required by this section.

(c) DETAILEE PROGRAM.—The Secretary shall—

(1) implement a Departmental detailee program to detail Departmental personnel to the National Archives and Records Administration for one year, for the purpose of—

(A) training and educational benefit for the Department personnel assigned so that they may better understand the policies, procedures, and laws governing the controlled unclassified information framework;

(B) bolstering the ability of the National Archives and Records Administration to conduct its oversight authorities over the Department and other Departments and agencies; and

(C) ensuring that the policies and procedures established by the Secretary remain consistent with those established by the Archivist of the United States; and

(2) in coordination with the Archivist of the United States, report to Congress not later than 90 days after the conclusion of

the first year of the program established under paragraph (1), on—

(A) the advisability of expanding the program on a government-wide basis, whereby other departments and agencies would send detailees to the National Archives and Records Administration; and

(B) the administrative and monetary costs of full compliance with this section.

(d) TERMINATION OF DETAILEE PROGRAM.—Except as otherwise provided by law, subsection (c) shall cease to have effect on December 31, 2012.

SEC. 210H. DEFINITIONS.

In this Act:

(1) CONTROLLED UNCLASSIFIED INFORMATION.—The term "controlled unclassified information" means a categorical designation that refers to unclassified information, including unclassified information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including unclassified homeland security information, terrorism information, and weapons of mass destruction information (as defined in such section) and unclassified national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))), that does not meet the standards of National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or National Archives and Records Administration policy requires safeguarding from unauthorized disclosure, special handling safeguards, or prescribed limits on exchanges or dissemination.

(2) CONTROLLED UNCLASSIFIED INFORMATION FRAMEWORK.—The term "controlled unclassified information framework" means the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of terrorism-related controlled unclassified information that originates in departments and agencies, regardless of the medium used for the display, storage, or transmittal of such information, as set forth in the President's May 7, 2008 Memorandum for the Heads of Executive Departments Regarding Designation and Sharing of controlled unclassified information (CUI), and in any relevant future executive memoranda, executive orders, or legislation.

(3) FINISHED INTELLIGENCE PRODUCT.—The term "finished intelligence product" means a document in which an intelligence analyst has evaluated, interpreted, integrated, or placed into context raw intelligence or information.

* * * * * * *

COMMITTEE CORRESPONDENCE

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 28, 2008

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and
Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Waxman:

Thank you for your letter regarding H.R. 6193, the "Improving Public Access to Documents Act of 2008," introduced by Congresswoman Jane Harman on June 5, 2008.

I appreciate your willingness to work cooperatively on this legislation. I acknowledge that H.R. 6193 contains provisions that fall under the jurisdictional interests of the Committee on Oversight and Government Reform. I appreciate your agreement to not seek a sequential referral of this legislation and acknowledge that your decision to forgo a sequential referral does not waive, alter, or otherwise affect the jurisdiction of the Committee on Oversight and Government Reform.

Further, I recognize that your Committee reserves the right to seek appointment of conferees on the bill for the portions of the bill that are within your jurisdiction, and I agree to support such a request.

I will ensure that this exchange of letters is included in the Committee's report on H.R. 6193 and in the *Congressional Record* during floor consideration of H.R. 6193. I look forward to working with you on this legislation and other matters of great importance to this nation.

Sincerely,

Bennie G. Thompson
Chairman

cc: The Honorable Nancy Pelosi, Speaker
The Honorable Peter T. King, Ranking Member
The Honorable John Sullivan, Parliamentarian

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
BRIAN HIGGINS, NEW YORK
JOHN A. YARMUTH, KENTUCKY
BRUCE L. BRALEY, IOWA
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
BETTY MCCOLLUM, MINNESOTA
JIM COOPER, TENNESSEE
CHRIS VAN HOLLEN, MARYLAND
MIKE QUIGLEY, NEW HAMPSHIRE
CHRIS HALL, MISSOURI, CONNECTICUT
DAN MAFFEI, NEW YORK
PETER WELCH, VERMONT
JACKIE SPEIER, CALIFORNIA

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

Majority (202) 225-5051
Minority (202) 225-5074
Minority (202) 225-5074

www.oversight.house.gov

TOM DAVIS, VIRGINIA
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
JOHN M. MCHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
DARRELL E. ISSA, CALIFORNIA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. MCHENRY, NORTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
BILL SALI, IDAHO
JIM JORDAN, OHIO

July 25, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson:

I am writing about H.R. 6193, the Improving Public Access to Documents Act of 2008, which the Homeland Security Committee ordered reported to the House on June 26, 2008.

I appreciate your effort to consult with the Committee on Oversight and Government Reform regarding H.R. 6193. In particular, I appreciate your willingness to work with me to move a governmentwide pseudo-classification bill, H.R. 6576, to the House floor so that H.R. 6193 and H.R. 6576 can be considered during the same week.

In the interest of expediting consideration of H.R. 6193, the Oversight Committee will not request a sequential referral of this bill. I would, however, request your support for the appointment of conferees from the Oversight Committee should H.R. 6193 or a similar Senate bill be considered in conference with the Senate.

Moreover, although the Oversight Committee has agreed to forgo a sequential referral of this measure, I believe it is important to reiterate my general concern about H.R. 6193 as it applies to the Department of Homeland Security.

H.R. 6193 creates procedures for the Department to follow in order to reduce the proliferation of unnecessary information classification. This is a commendable goal, however, investigations by the Oversight Committee have demonstrated that there has been a proliferation of pseudo-classification designations such as "sensitive but unclassified" or "for official use only." In my view, any legislation addressing information control designations should be implemented on a government-wide basis.

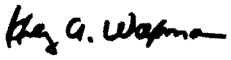
The Honorable Bennie G. Thompson
July 25, 2008
Page 2

Again, thank you for considering my concerns about H.R. 6193. I look forward to working with you to reduce the serious problem of pseudo-classification of information throughout the federal government.

This letter should not be construed as a waiver of the Oversight Committee's legislative jurisdiction over subjects addressed in H.R. 6193 that fall within the jurisdiction of the Oversight Committee.

Please include our exchange of letters on this matter in the Homeland Security Report on H.R. 6193 and in the Congressional Record during consideration of this legislation on the House floor.

Sincerely,



Henry A. Waxman
Chairman

cc: Tom Davis
Ranking Minority Member