REINING IN EXCESSIVE SECRECY: RECOMMENDATIONS FOR REFORM OF THE CLASSIFICATION AND CONTROLLED UNCLASSIFIED INFORMATION SYSTEMS

A REPORT BY THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

JULY 16, 2009

The Constitution Project
1200 18th Street, NW, Suite 1000
Washington, DC 20036
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org
www.constitutionproject.org

REINING IN EXCESSIVE SECRECY: RECOMMENDATIONS FOR REFORM OF THE CLASSIFICATION AND CONTROLLED UNCLASSIFIED INFORMATION SYSTEMS*

INTRODUCTION

The fundamental principles of openness, public debate, and accountability, central to our democracy, are most vulnerable when our nation's security is threatened. It is difficult during times of threats to our nation's security for our leaders to find the ideal balance between accountability and security; however, recent history reveals we have repeatedly failed to find the true balance. We have too often favored secrecy and lack of transparency at the expense of openness and accountability. This pattern persists today, as excessive secrecy and over-classification remove vast amounts of information from public scrutiny, shielding misconduct and impeding oversight.[1]

On May 27, 2009, President Barack Obama issued a Memorandum for the Heads of Executive Departments and Agencies, "Classified Information and Controlled Unclassified Information."[2] The Memorandum seeks recommendations on how best to reform the federal government's systems both of classification and of designation of sensitive information outside the classification sphere. This effort should serve as a call to reinforce core constitutional principles including checks and balances and accountability to the public. Through this report, the Constitution Project urges the Assistant to the President for National Security Affairs and the Interagency Task Force on Controlled Unclassified Information (CUI) to heed that call. The Constitution Project is an independent, nonprofit organization that seeks to develop consensus solutions to difficult legal and constitutional issues. We accomplish this through constructive dialogue across ideological and partisan lines, and through scholarship, activism, and public education efforts.

For the following reasons, we, the undersigned members of the Constitution Project's bipartisan Liberty and Security Committee, offer the recommendations below for revising Executive Order 12958, as amended (Classified National Security Information), and for reforming the CUI Framework, in order to ensure that we properly safeguard constitutional principles, national security, privacy, and other important interests. Our recommendations are informed by the history and challenges attendant to both the classified information and CUI systems. Specifically, over-classification of documents inhibits government transparency while at the same time weakening the classification system. It also needlessly increases the cost of accessing and using information even within government due to required security and management obligations. The end result is a flawed exercise that neither permits public accountability nor sufficiently protects national security. Similarly, the present CUI system lacks the standards or procedures necessary for ensuring appropriate designation and minimizing barriers to information sharing both among government bodies and with the public, ultimately compromising the safety of our citizens.

---

* The Constitution Project sincerely thanks David Medine and Anne Sherwood of the law firm WilmerHale for their extensive researching and drafting work on this statement as well as a background report for committee members, and for their work in guiding committee members to consensus on these issues.

1 *See Restoring the Rule of Law: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong., at 1 (Sept. 16, 2008) (statement of Steven Aftergood, Federation of American Scientists), *available at* http://feingold.senate.gov/ruleoflaw/testimony/aftergood.pdf.

2 74 Fed. Reg. 26277 (June 1, 2009).

The constitutional stakes are high. Because the impediments to information sharing run not only among agencies but also among government branches, the constitutional system of checks and balances that traditionally protects individual rights and national security has been weakened. What is more, agencies' over-classification and over-designation have threatened First Amendment rights guaranteeing freedom of the press, which encompasses the ability to investigate and report on government actions. Excessive government secrecy has prevented public accountability by obstructing citizens' ability to seek disclosure of government-held information. This collective lack of transparency causes mistrust in government that further undermines our democracy.

The amount of information improperly withheld from public scrutiny is staggering. Testifying before Congress, government officials have estimated that as much as fifty percent of defense information may be improperly classified.[3] A 2006 audit report of the Information Security Oversight Office (ISOO) found that at least one out of three of more than 25,000 previously open records had been improperly re-classified.[4] Over-classification of this scale is not only problematic, but also dangerous. Transparency helps ensure our actual security, and the records that chronicle the actions of government officials provide the accountability necessary for a healthy and vital democracy.

In order to protect these constitutional values, the government's efforts should focus on two main objectives: (1) increase information sharing among agencies and across branches of government in order to better protect our national security, and (2) increase disclosure of government-held information to the public and other branches of government, in order to enhance government transparency, improve accountability, and protect liberty interests. We believe that the government can accomplish both of these goals by adopting the recommendations set forth below.

I. OVER-CLASSIFICATION

The unchecked over-classification of information hinders effective national security policy by slowing the flow of information among government bodies and frustrating oversight and accountability. Traceable to outdated Cold War "cultural biases against information sharing,"[5] excessive and improper over-classification has repeatedly interfered with decision-making processes by "walling in" information from necessary government actors, resulting in poor or incomplete analysis. Excessive secrecy and lack of transparency have also eroded citizens' trust in their government, erecting unnecessary barriers between the public and the actions of the Executive Branch.

The harmful effects of over-classification are well-known and hardly new. Our history has repeatedly shown that excessive secrecy subverts government accountability and allows government officials to conceal illegalities. Perversely, it also undermines national security by unnecessarily increasing the volume of classified information and augmenting the risk that

---

[3] *See Too Many Secrets: Overclassification as a Barrier to Information Sharing: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the H. Comm. on Government Reform*, 108th Cong., at 82 (Aug. 24, 2004) (statement of Carol A. Haave, Deputy Secretary of Defense for Counterintelligence and Security); Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12 (acknowledging "too much material is classified across the federal government as a general rule").

[4] *See The Media's Role and Responsibilities in Leaks of Classified Information: Hearing Before the H. Permanent Select Comm. on Intelligence*, 109th Cong., at 1 (May 26, 2006) (statement of Meredith Fuchs, General Counsel, National Security Archive).

[5] Lawrence J. Halloran, *Briefing Memorandum for the Hearing "Emerging Threats: Overclassification and Pseudo-Classification,"* Memorandum for the Members of the Subcommittee on National Security, Emerging Threats, and International Relations, at 2 (Feb. 24, 2005).

sensitive documents will be mishandled or released.[6] It is as true now as it was in 1970, when Justice Potter Stewart wrote his concurring opinion in the *Pentagon Papers Case*, that "the only effective restraint upon executive policy and power . . . may lie in an enlightened citizenry—in an informed and critical public opinion which alone can [] protect the values of democratic government."[7]

More recently, in its assessment of information security policies in the years preceding the attacks of September 11, 2001, *The Final Report of the National Commission on Terrorist Attacks Upon the United States* (*9/11 Commission Report*) found that existing "security requirements nurture[d] overclassification and excessive compartmentation of information among agencies."[8] The 9/11 Commission also recognized that this trend deprived intelligence and law enforcement of a potent weapon against terrorism: an alert and well-informed American public.[9] These findings motivated the Commission to recommend the creation of a decentralized "trusted information network" that would facilitate interagency communication and information sharing.[10]

Despite the Commission's findings, recent years have seen a trend towards *increased* government secrecy under both national security classifications—i.e., "confidential," "secret," or "top secret"[11]—and "sensitive but unclassified" (SBU) designation frameworks. Security classification has surged dramatically since September 11, 2001, reaching an all-time high of 23 million classification decisions in 2007, nearly triple the number in 2001. Recent changes to Executive Order 12958, which governs the national security classification system, have encouraged greater secrecy.[12] By 2005, government departments and agencies classified documents at the rate of 125 per minute, generating considerable costs to ultimately have them reviewed for declassification.[13]

The direction of significant funds and attention towards unneeded secrecy has left the National Archives and Records Administration (NARA)—tasked with processing declassified documents for release—with insufficient resources to do its job. A small group of executive branch agencies possess largely unchecked power to create and hold secrets in the federal government. These agencies often fail to consider significant public interests in release of certain classified records

---

6 *See Over-classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information: Hearing Before the Subcomm. On Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong., at 3 (June 28, 2007) (statement of Suzanne E. Spaulding, Principal, Bingham McCutchen Consulting Group LLC). Suzanne Spaulding explained this problem, noting:

> It may seem counterintuitive to some, but avoiding over-classification is essential to protecting vital national security secrets. Those handling classified documents will have greater respect for that "Top Secret" stamp if they know that things are only classified when their disclosure would truly harm national security. When things are classified whose disclosure clearly would not harm national security, it tempts some individuals to believe that they can decide what is really sensitive and what is not.

7 *New York Times Co. v. United States*, 403 U.S. 713, 728 (1971) (Stewart, J., concurring).

8 The Final Report of the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, at 417 (July 2004).

9 *See, e.g., id.* at 276, 383.

10 *Id.* at 418.

11 *See* Lawrence J. Halloran, *Memorandum for the Hearing "Emerging Threats: Overclassification and Pseudo-Classification,"* at 3 (Feb. 24, 2005) (noting "[s]ecurity concerns after the September 11th attacks prompted some departments and agencies to increase the type and volume of information shielded by public view by *Confidential*, *Secret* or *Top Secret* markings").

12 *See Classification of National Security Information and Its Implications for the Intelligence Community: Hearing Before the Subcomm. on Intelligence Community Management of the H. Permanent Select Comm. on Intelligence*, at 7 (July 12, 2007) (statement of Meredith Fuchs, General Counsel, National Security Archives) (citing 2003 modifications).

13 *See* Editorial, *The Dangerous Comfort of Secrecy*, N.Y. Times, Jul. 12, 2005, at A20. In fiscal year 2008, declassification alone cost agencies $43 million. Information Security Oversight Office, National Archives and Records Administration, *Fiscal Year 2008 Report on Cost Estimates for Security Classification Activities*, at 3 (2009).

or the damage to government operations and national security created by barriers to information sharing. They have reclassified publicly released records with abandon and fought efforts to declassify non-sensitive records.

II. CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Numerous federal agencies, using over 100 types of labels, have been designating information which does not qualify for national security classification as *sensitive but unclassified* (SBU) or *controlled unclassified information* (CUI), in a parallel often non-statutory system. There are valid reasons why documents that do not meet the criteria under the classification system described above may still be sensitive and need to be controlled for a limited period. For example, government agencies may legitimately wish to restrict access to law enforcement reports that do not involve classified national security information, such as a plan for handling a particular local threat or public event, so that any people planning disruptions do not gain access to the law enforcement plans ahead of time. However, the current SBU or CUI system lacks any clear standards or accountability and has often undermined the ability to share such information with other agencies or disclose it to the public. In fact, the lack of uniformity and uncertain status of CUI have been counterproductive, deterring use and sharing with law enforcement or intelligence agencies that would benefit from the information, as well as limiting public access and accountability and thwarting Congressional oversight.

In his May 27, 2009 memorandum, President Obama called for "further[ing] and expedit[ing]" the implementation of a new CUI Framework for the uniform handling of CUI, and he created the Interagency Task Force on CUI.[14] Its objective is:

> to review current procedures for categorizing and sharing SBU information in order to determine whether such procedures strike the proper balance among the relevant imperatives. These imperatives include protecting legitimate security, law enforcement, and privacy interests as well as civil liberties, providing clear rules to those who handle SBU information, and ensuring that the handling and dissemination of information is not restricted unless there is a compelling need.

The lack of clarity surrounding SBU, CUI, and similar designations is an obstacle to recommending constructive change. The vagueness of the concepts and discrepancies among agency practices makes discussion about "CUI" difficult. Yet, the President's call for reform *is* clear, and so is the government's commitment to using CUI controls. Public participation in the reform process is necessary to address that imprecision and to establish a transparent CUI system.

Therefore, to assist the Task Force with this goal, we detail here the history and status of CUI, and we propose to the Presidential Task Force a number of recommendations to reform the CUI process that will promote openness and accountability as well as advance important governmental interests.

A. Background

Simply put, SBU and similar labels—the precursors to the new "CUI" label—designate information that does not meet the standards for classification, but is deemed sensitive enough

[14] President Barack Obama, Memorandum of May 27, 2009, *Classified Information and Controlled Unclassified Information*, Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 26277, 26278 (June 1, 2009).

to be "controlled" by the labeling agency. The Congressional Research Service (CRS) reports that federal agencies started using the term "Sensitive But Unclassified" as early as the late 1970s.[15] Since the 1980s, agencies have used official classification categories, but have also regularly used various designations to control access to unclassified information deemed too sensitive for unrestricted access. Such information may include "privacy data, law enforcement information, health information, and information exempt from disclosure under the Freedom of Information Act (FOIA), and 'sensitive' information,"[16] or proprietary data such as corporate trade secrets submitted to a government agency. As a 2004 CRS report explained, "'sensitive but unclassified' [came] to be used to encompass information subject to control pursuant to the Computer Security Act [of 1987], as well as information determined to be exempt from disclosure under [FOIA]."[17] Whatever the justifications used, control has been authorized by statute or regulation in only some circumstances. In many instances, agency employees have controlled information based on no clear legal authority.[18]

The George W. Bush Administration adopted the CUI designation because it believed the lack of a uniform system controlling SBU slowed the sharing of information among government agencies.[19] Indeed, years of disparate systems of designation created barriers to information sharing. The problem coalesced in the grave communication failures that contributed to the events of September 11, 2001: Government investigations into the attacks concluded that "excessive secrecy interfered with the detection and prevention of the attacks."[20] Those information sharing problems were exacerbated in the attack's aftermath as agencies created various new SBU designations in an attempt to safeguard information deemed to have the potential to be used against the United States.[21] As a result, government secrecy and over-classification increased.

To counteract the perceived negative effects of over-classification, Congress passed and President Bush signed the Intelligence Reform and Terrorism Prevention Act (IRTPA) in 2004. IRTPA required the President to develop an Information Sharing Environment (ISE) to facilitate the sharing of terrorism and homeland security information across levels of government as well as with important private actors and foreign governments. To support the ISE, President Bush issued a December 2005 memorandum detailing information sharing guidelines among several

---

[15] Genevieve J. Knezo, Congressional Research Service, *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*, at 10 (2006).

[16] Genevieve J. Knezo, Congressional Research Service, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, at 16 (2004).

[17] *Id.*

[18] As some studies have found, the designations are not rooted in statutes or regulations, but rather are based only on department or agency policy. *See, e.g.*, OpenTheGovernment.org, *Secrecy Report Card 2008: Indicators of Secrecy in the Federal Government* 16 (2008), *available at* http://www.openthegovernment.org/otg/SecrecyReportCard08.pdf. In 2004, the Library of Congress cataloged the laws and regulations governing SBU information. Library of Congress, Federal Research Division, *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information* (Sept. 2004). The report detailed a complex matrix of presidential and national security directives, laws applicable to all government agencies, and laws and regulations governing individual agencies.

[19] *See The Over-Classification and Pseudo-Classification of Governmental Information: The Response of the Program Manager of the Information Sharing Environment: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (Apr. 26, 2007) (statement of Ambassador Ted McNamara, Program Manager, Information Sharing Environment), *available at* http://www.ise.gov/docs/speeches/HHSC-20070426-%20McNamara%20Testimony.pdf.

[20] *Overclassification and Pseudo-classification: The Impact on Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment, H. Comm. on Homeland Security*, 110th Cong., at 3 (Mar. 22, 2007) (statement of Meredith Fuchs, General Counsel, National Security Archive).

[21] Press Release, OMB Watch, *White House Issues Memo on Controlled Unclassified Information* (May 13, 2008), *available at* http://www.ombwatch.org/print/3692.

key government departments and directing federal departments and agencies to recommend standardized SBU procedures for terrorism-related information.[22]

B. The First Steps Toward a CUI Framework

On May 7, 2008, President George W. Bush issued a memorandum with the stated purpose of "adopt[ing], defin[ing], and institut[ing] 'Controlled Unclassified Information' (CUI) as the single categorical designation henceforth throughout the executive branch for all information within the scope of that definition . . . ."[23] The memorandum established a uniform designation for information outside the scope of the National Security Classification framework for intelligence, defense, and foreign policy matters governed by Executive Order 12958,[24] but still considered "pertinent to [U.S.] national interests" or to "important interests outside the federal government." The new CUI designation was also intended to replace over 107 different unique markings and 130 different labeling or handling processes used at various agencies to control records previously known collectively as "Sensitive But Unclassified" information (SBU).[25]

As defined in President Bush's May 2008 memorandum, CUI:

> refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12598 [but is nevertheless] 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 policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.[26]

President Bush's May 2008 memorandum also created a framework for uniform handling of CUI (CUI Framework), but limited this Framework to "terrorism-related information" as defined by the 9/11 Commission Act of 2007, homeland security information, and law enforcement information relating to terrorism. Under the CUI Framework, CUI can be categorized under three different combinations of safeguarding procedures and dissemination controls: (i) Controlled with Standard Dissemination; (ii) Controlled with Specified Dissemination; and (iii) Controlled Enhanced with Specified Dissemination. Agencies are barred from creating new CUI categories unless they are prescribed by the National Archives and Records Administration (NARA) in its capacity as "Executive Agent."

---

[22] President George W. Bush, *Guidelines and Requirements in Support of the Information Sharing Environment*, Memorandum for the Heads of Executive Departments and Agencies (Dec. 16, 2005).

[23] President George W. Bush, *Designation and Sharing of Controlled Unclassified Information (CUI)*, Memorandum for the Heads of Executive Departments and Agencies (May 7, 2008), *available at* http://www.archives.gov/cui/documents/designation_cui.pdf.

[24] Exec. Order No. 12958, as amended, 68 Fed. Reg. 15315 (Mar. 28, 2003).

[25] National Archives and Records Administration, *Controlled Unclassified Information "Fact Sheet"* (Oct. 16, 2008).

[26] There are other definitions of CUI, such as the following found in proposed legislation:

> 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.
>
> Improving Public Access to Documents Act of 2008, H.R. 6193, 110th Cong. (2008).

That memorandum also makes clear that the new CUI designation encompasses all information previously covered under SBU categorizations. Additionally, it sets forth requirements necessary for information to be designated CUI. Information may be designated CUI if "(a) a statute requires or authorizes such a designation; or (b) the head of the originating department or agency, through regulations, directives, or other specific guidance to the agency, determines that the information is CUI."[27]

The memorandum also clarifies that information may *not* be designated CUI: (i) in order to conceal violations of law or administrative error, prevent embarrassment to the federal government, or facilitate other improper purposes; (ii) if it is information required to be made available to the public; or (iii) it has already been released to the public under proper authority.[28] These definitions and requirements are not altered by President Obama's May 2009 memorandum.

Full implementation of the CUI Framework presently is scheduled to be completed by 2013. In the interim, some departments have said they will not switch to any new CUI marking system until a national level interagency policy has been issued. The Department of Defense, for example, has expressed a policy of "strict adherence" to existing information policy guidance and designations, such as "For Official Use Only" (FOUO), SBU, and DoD Unclassified Controlled Nuclear Information, until a comprehensive national policy is in effect.[29]

Indeed, President Obama's May 2009 memorandum recognizes that the present CUI Framework requires further revision:

> In the absence of a single, comprehensive framework that is fully implemented, the persistence of multiple categories of SBU, together with institutional and perceived technological obstacles to moving toward an information sharing culture, continue to impede collaboration and the otherwise authorized sharing of SBU information among agencies, as well as between the Federal Government and its partners in State, local, and tribal governments and the private sector.[30]

A variety of concerns and consequences must be addressed in order to ensure the CUI Framework meets constitutional standards and preserves the principles of transparency, openness, and accountability. We address those concerns and consequences below.

C. Consequences of Designation

1. Keeping Truly Sensitive Information Protected

Overuse of the CUI designation has real consequences for the protection of truly sensitive information. As has been noted in the classification context, "overclassification and unneeded secrecy . . . undermine the effort to keep truly sensitive information secret,"[31] and the same concerns apply here. Because preventing over-designation is one of the hurdles the Task Force must overcome with respect to CUI, it should recommend a CUI Framework that will strengthen sensitivity to designations by limiting their scope, applicability, and duration.

---

[27] President Bush May 2008 Memorandum, *supra* note 23.
[28] *Id.*
[29] Under Secretary of Defense, *Memorandum on Clarification of Current DoD Policy on Controlled Unclassified Information (CUI)* (Apr. 7, 2009).
[30] 74 Fed. Reg. at 26278.
[31] Fuchs July 2007 testimony, *supra* note 12, at 4. "'For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or careless, and to be manipulated by those intent on self-protection or self-promotion.'" *Id.* at 4-5 (quoting *New York Times Co.*, 403 U.S. at 729 (Stewart, J., concurring)).

2. Facilitating or Frustrating Information Sharing Within the Government

In their present incarnation, SBU, CUI, and other agency-assigned labels still frustrate information sharing, creating an impediment to protecting national interests. The lack of uniform standards prevents individuals in one agency from understanding the designations in another, resulting in confusion about their proper use and handling. The tendency to over-designate and under-share should be resisted, as it impedes the flow of information.[32] Without structured, system-wide change that creates universally used and understood procedures, a new CUI Framework will become the same impediment as the failed agency-specific approach. Part of the challenge will be to reconcile different agencies' sensitive-information cultures[33] and equally difficult may be determining how to handle materials still designated under each agency's pre-CUI systems.[34]

Ideally, however, a CUI Framework should *facilitate* information sharing by allowing agencies to flag information that should be shared with other government entities. By standardizing systems and procedures, it should also relieve uncertainty about who should have access to certain information and how to handle that information once access is given.

3. Facilitating or Frustrating Information Sharing with the Public

a) Affecting the Disclosure of Information under FOIA

Government transparency and accountability are vital to a functioning democracy. The First Amendment guarantees freedom of the press, and part of that freedom is the ability to investigate and report on government actions. To serve as an effective external government watchdog, the media require access to government information, particularly information that the government would prefer not be seen by the public. Tom Curley, the President and CEO of the Associated Press noted that "If you leave FOIA defenseless, agencies will continue too often to take the risk-free path—the easy path—and just say no. And they're all the more likely to do it when something has gone wrong that the public really, really needs to know about."[35]

To accomplish the goal of transparency, the government should be engaged in rigorous scrutiny of what information falls under FOIA to increase the amount of information disseminated. Some agencies may rely on SBU designations as proxies for FOIA exemptions. Those agencies are substituting a designation determination (perhaps conducted by an employee of any level, or even by a contractor, with little or no accountability for his or her actions) for an agency's statutory obligation to conduct a full review under FOIA to determine whether the specific piece of information is exempt from a public request for disclosure.

These designations should never be presumed to be a substitute for a full and proper FOIA evaluation. Because SBU designations—or the newer CUI designation—are *handling* instructions, they serve a purpose separate and apart from a FOIA review, even if the relevant considerations for each determination may overlap. What is more, because a designation may be meant to reflect a time-sensitive, and therefore short-lived concern, use of the designation in response to a later FOIA request may be especially misplaced.

---

[32] *See* H.R. 6193, 110th Cong. (2008).

[33] *See* Spaulding testimony, *supra* note 6, at 6.

[34] *See* Letter from Senator Lieberman and Senator Collins to Michael Chertoff, Secretary, U.S. Dep't of Homeland Security (May 1, 2007), *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=a2390230-8a40-4cfa-8e82-22c68664587a&Region_id=&Issue_id= (asking about the re-labeling of SBU-designated materials).

[35] *Open Government: Reinvigorating the Freedom of Information Act: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (Mar. 14, 2007) (statement of Tom Curley, President and CEO, Associated Press).

Finally, history demonstrates a natural tendency on the part of government agencies toward over-classification and over-designation. That threat remains even under a new CUI Framework. To fully protect the public's interests and its First Amendment rights, a full FOIA review must be conducted independent of—and without reliance on—a CUI designation. In order to correct the failures under the present system, the new CUI Framework must clarify this separation between FOIA and CUI markings.

b) Affecting the Availability of Information Pursuant to Discovery

Some information presently designated sensitive is not subject to discovery in civil litigation. For instance, according to a resource document issued by the Federal Transit Administration, information designated "Sensitive Security Information" is, by law, not discoverable.[36] Such exemptions may serve important security and safety goals. However, where no such authority is in place, the CUI Framework should clarify that documents marked CUI are not presumptively exempt from discovery.

c) Helping or Hindering Public Accountability

The greater the over-designation problems, the more government accountability is inhibited. The greater the level of secrecy around the designation process, the more likely the public is to mistrust even the legitimate and appropriate use of security controls on any information. The Executive Branch has rightly recognized that the CUI designation can be an important tool for protecting sensitive information. But CUI's power as a tool to protect information must be balanced by safeguards to ensure that only proper information is designated. Therefore, if it is to be effective within government and regarded as legitimate by those outside government, the CUI Framework must introduce both internal mechanisms and external oversight to ensure accountability.

4. Applying Beyond the Terrorism Context

Because President Bush's 2005 and 2008 Memoranda targeted sensitive information to be shared through the ISE, pursuant to IRTPA, the CUI designation presently appears to be limited only to terrorism-related information.[37] Under such an interpretation of CUI, certain information previously considered SBU would remain outside the CUI Framework. Therefore, President Obama has asked the Task Force to submit recommendations on whether the scope of the CUI Framework should be broadened to include all SBU information.

The exclusion of a substantial amount of SBU non-terrorism related information from the CUI Framework will leave much information unaddressed.[38] Not only will it be "difficult, if not impossible, to segregate 'terrorism-related information' from other kinds of information,"[39] but many of the same information-sharing and accountability concerns will remain for those sets of

---

[36] U.S. Dep't of Transportation, Federal Transit Administration, *Sensitive Security Information (SSI): Designation, Markings, and Control*, at 9 (Mar. 2009). Pursuant to section 525(d) of the Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, 120 Stat. 1355 (2006), information designated "SSI" by the Transportation Security Administration is not discoverable in civil litigation absent the showing of substantial need and undue hardship, and a judicial protective order.

[37] *See, e.g.*, OMB Watch, *Controlled Unclassified Information: Recommendations for Information Control Reform*, at 6 (July 2009). However, it is not entirely clear from the language of Presidents Bush's 2008 order that he intended such a limitation, particularly because that Memorandum stated only that the CUI designation would "include[]" information that had been designated SBU under the ISE, but it did not expressly limit the designation to that information. Others have probed whether President Bush's 2005 order reached information housed in every government agency. For instance, Senators Lieberman and Collins noted that because some agencies do not fall under the authority of the officer designated to oversee the ISE, the ISE Program Manager, all agencies may not be governed by the standardized system. *See* Lieberman Letter, *supra* note 34.

[38] *See* Press Release, OMB Watch, *White House Issues Memo on Controlled Unclassified Information* (May 13, 2008), *available at* http://www.ombwatch.org/print/3692.

[39] OMB Watch, *supra* note 37, at 7.

sensitive information deemed to fall outside the terrorism context.[40] Provided that our recommendations for reforming the CUI Framework are adopted, we further recommend that the new CUI Framework should not be limited to terrorism-related information.

* * * *

As we previously have stated, the CUI Framework should achieve two main objectives: (1) increase information sharing among agencies and branches of government, and (2) increase disclosure of government-held information to the public, in order to enhance government transparency and protect liberty interests. These goals are not mutually exclusive but, rather, are complementary in a well-functioning democracy. The challenge will be to craft a CUI Framework that simultaneously serves both ends. We urge the Task Force and the President to follow our recommendations outlined below in formulating the new Framework.

RECOMMENDATIONS

We, the undersigned members of the Constitution Project's Liberty and Security Committee, make the following recommendations.

I. RECOMMENDATIONS ON THE PROBLEM OF OVER-CLASSIFICATION

A. New Executive Order on Classification

Endorse Presumption of Openness

1. Executive Order 12958 has been amended over time to increase secrecy, often counter to the goals of openness and accountability. The President should issue a new executive order on classification, pledging accountability in the classification process. The new order should establish a new framework for designating information with a presumption in favor of openness that limits classification only to information that must be protected to avoid harm to national security, with clear standards and procedures for proper classification.

2. The order should include a presumption in favor of lower level classifications, or declassification, such that decisionmakers resolve doubts by applying the lower classification level or no classification.

3. The order should eliminate current Section 1.1(c), which creates a presumption that foreign government information is classified. Such information is already subject to classification as one of the categories noted in Section 1.4 and there is no need for such a presumption.

4. The order should clarify that information "may" be classified if standards are met, but that the classifier has discretion. Although Section 1.1(a) clearly states that for original classifications, information "may be originally classified under the terms of this order only if all of the following conditions are met," this is undermined by the descriptions of available classification levels which include the term "shall." Specifically, in Section 1.2(a), which sets forth the available classification levels, each

[40] *See* Beverley Lumpkin, The Project on Government Oversight, *Simplifying the Alphabet Soup* (Jan. 23, 2008), *available at* http://pogoblog.typepad.com/pogo/2008/01/simplifying-the.html (citing concerns that some agency-specific markings will continue to be used).

category (i.e. Top Secret, Secret, and Confidential) should state that it "applies to" the described information, rather than that it "shall be applied to" such information.

5. Only information meeting the definitions of Top Secret, Secret, and Confidential in Section 1.2 should be permitted to be classified. Section 1.2 states:

> (1) ''Top Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
>
> (2) ''Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
>
> (3) ''Confidential'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

   The order should expressly prohibit the classification of material that does not meet one of these definitions.

Weigh Public Interest in Classification/Declassification Decisions

6. The revised Executive Order should require consideration of the public interest before information is classified.

7. The new executive order should include a balancing test that would require the government to weigh the public value of the information in declassification decisions. Specifically, Section 3.1(b) of EO 12958 should be amended to delete the current first sentence and alter the next sentence so that it reads: "Information may continue to be classified only if the need to protect such information outweighs the public interest in disclosure of the information." Also, Section 3.5(c) should be revised so that the first sentence is expanded as follows: "Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order, or where the public interest in disclosure outweighs the need to protect the information." In the second sentence of this section, "authorized and warranted" should be changed to "required," so that the sentence would read "They shall release this information unless withholding is otherwise required under applicable law."

Aid Sharing of National Security Information

8. To ensure national security information may be shared among the necessary parties, the government should create clear and effective processes for sharing classified information.

Provide Accountability and Limits on Classification

9. The Executive Order should explicitly prohibit abuse of classification markings.

10. The order should decrease the timeframes for automatic declassification. Section 1.5(b) presently states that "[i]f the original classification authority cannot determine an earlier specific date or event for declassification," information shall be automatically declassified after 10 years, unless the sensitivity of the information requires longer classification, in which case it shall be automatically declassified after a period up to 25 years. The lower time limit of this automatic declassification range should be decreased from 10 years to 5 years, and the upper limit should be decreased from 25 years to 20 years.

11. The order should include methods of systematization and improvement of the process for declassification of *historical records* and institute stricter standards for reclassification.

12. The order should decrease the time period for automatic declassification under Section 3.3 from 25 years down to 20 years, and strengthen the requirements for seeking an extension of this time period. Section 3.3(b) currently permits an extension of the classification time period beyond 25 years for information the "release of which could be expected to" result in one of various listed harmful results. This standard should be changed to require that the release of the information "is significantly likely to" lead to the listed harmful results.

13. The existing classification order provides for "derivative classification" by personnel who are not required to possess original classification authority to "carry forward" the original classifications into summaries, discussions, and other documents that are created from or rely upon such classified material. Since such derivative classifications may be made by personnel who lack the training and authority of original classifiers, the order should require greater oversight of the derivative classification process. Specifically, the order should require that derivative classifications must be reviewed and approved by a person with original classification authority within 5 years of the derivative classification marking in order to retain their classification.

14. The order should establish new mechanisms for oversight of the classification system to guarantee accountability and transparency. The order should be revised to strengthen the role of the Director of the Information Security Oversight Office (ISOO) by replacing "have the authority to" with "regularly" in the first sentence of Section 5.2(b)(4), so that that provision would read "regularly conduct on-site reviews of each agency's program established under this order, and require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities." The order also should require regular audits and reporting by the Inspectors General (IGs) of each federal agency that maintains classified materials, or by some other external oversight authority.

Support Legislation to Limit Classification

15. It is vital that all branches of government come together to address the problems of over-classification and secrecy. The President should work with Congress to ensure passage of legislation designed to reduce over-classification.

B. Government Review of Classification

Create Agency-Level Review of Classification

16. Each federal agency that classifies information should periodically conduct a detailed public review of its classification practices. This review should include a public notice and comment period and publication in the Federal Register. The review should have the objective of reducing national security secrecy to the essential minimum and declassifying all information that has been classified without a valid national security justification, consistent with the declassification standards laid out above.

C. Legislative Action

Strengthen Congressional Oversight of the Classification Process

17. Congress should be rigorous in its oversight of the classification processes at each agency and at all levels of government. It should pass legislation designed to reduce over-classification.

Pass an Omnibus Historical Records Act

18. To increase government openness, Congress should pass an omnibus Historical Records Act that would accelerate declassification of historical records. This would ensure that historically significant information is declassified in a timely manner. The HRA would provide government transparency by decreasing unnecessary secrecy as well as increase public access to historical records.

II. Recommendations for Reforming the CUI Framework

A. Promote Openness and Limit Secrecy Within the Government and With the Public

Endorse Presumption of Openness

1. When considering whether to identify information as sensitive but unclassified, the traditional practice throughout the agencies has been to control information unless there exists a compelling reason for sharing. The National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) found that "agencies uphold a 'need-to-know' culture of information protection rather than promoting a 'need to share' culture of integration." This practice should be reversed to create a *presumption of openness*. This will serve the twin goals of promoting information sharing to protect the nation and increasing government accountability.

Adopt Legislation to Formalize Treatment of Information

2. The 2008 Bush Memorandum stated that the CUI marking should be given to information that 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 policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination."

To limit inclusion to appropriately identified information, clear guidance should be provided to government agencies with regard to the types of information that should be deemed CUI. Congress should define what constitutes CUI and create standards for when disclosure should be restricted because the information compromises privacy, security, or other legitimate interests. Outside of those necessary areas, there should be a presumption that the information does not need to be marked as controlled.

Enforce Portion Marking for CUI

3. The 2008 Bush Memorandum specifies that "[m]aterial that contains both CUI and non-CUI information, or that contains multiple categories of CUI, should be marked accordingly by portions such that those categorical distinctions are apparent." This requirement for portion marking should be continued and enforced.

Increase Access to CUI Materials Across Agencies and to Congress

4. A key shortcoming of the present identification system is the lack of guidance as to when CUI can be shared, and with whom. This uncertainly can undermine the value of sensitive information and deter appropriate sharing. Employees in and contractors for each agency should be given clear guidance and training in the appropriate use and sharing of CUI. The CUI Framework should require access to CUI materials to achieve a high level of openness across agencies and to Congress.

Adopt a Requirement that CUI Designations Sunset after a Specified Number of Years

5. Just as Executive Order 12958 sets a timeline for automatic declassification, the CUI Framework should incorporate provisions for automatic de-control of CUI-designated information. The CUI Framework should specify that, when no earlier date or event for de-control is determined, then CUI identifications sunset after a maximum number of years. We recommend a range for such sunset periods of between 2 and 10 years, with the 10 year period reserved for the most sensitive documents. Reinstatement of a CUI identification should require a separate review.

De-link CUI Identification from FOIA

6. Under the 2008 Bush Memorandum, "CUI markings may inform but do not control the decision of whether to disclose or release the information to the public, such as in response to a request made pursuant to the Freedom of Information Act (FOIA)." However, allowing agencies to consider CUI markings for FOIA purposes will improperly limit public access to information. Agencies should be required to undertake an independent analysis of whether any FOIA exemption applies. In making this assessment, agencies should give **no** weight to any CUI markings.

Accelerate CUI Framework Implementation Schedule

7. The President should require implementation of the CUI Framework no later than December 31, 2011. The Task Force should recommend an interim plan for treatment of CUI to cover the time period until the final Framework is implemented.

Make the Task Force's Recommendations Public and Seek Public Comment

8. Public feedback throughout the reform process is necessary to ensure accountability of the CUI regime. The proposed CUI Framework therefore should be published in the Federal Register for public notice and comment before it is adopted in final form.

Do Not Limit the CUI Framework to Terrorism-Related Information

9. Provided that these recommended reforms for the CUI Framework are adopted, the CUI Framework should not be limited to terrorism-related information within the information sharing environment. Rather, it should be applied beyond the terrorism context in order to standardize the identification, marking, and handling of all sensitive but unclassified (SBU) information. Government-wide standards for handling all sensitive information will further promote transparency and accountability.

B. Promote Accountability Within the Executive Branch

Require Personal Identifiers to Facilitate Reviews

10. The government should require the use of personal identifiers, so that the individual making CUI markings can be identified from the markings. The government should also require CUI markings to specify the purpose of the marking (which could be a code), the date of the marking, and the statutory or Executive Order authority for the designation. Such markings would facilitate oversight reviews to determine whether markings comply with applicable standards and the presumption of openness, and whether any policy or training modifications are needed.

Standardize Procedures for Handling CUI

11. To safeguard information designated as CUI, the government should establish protocols for identifying, using, storing, sharing, and properly destroying CUI materials. To prevent excessive CUI marking and over-inclusion, there should be procedures in place to limit such authority to only specially trained government officials.

Prohibit Use of CUI Marking for Improper Purposes

12. The government should ensure that CUI does not become a catch-all identification for information that does not meet classification standards, but that government actors nevertheless would prefer not be made public. Improper purposes include concealing embarrassing or illegal agency actions, or inefficiency.

Provide Whistleblower Protection

13. To promote the appropriate use of CUI controls, whistleblowers who bring to light government non-compliance with CUI guidelines should be protected from reprisal.

C. Provide For Oversight and Accountability by Congress and with the Public

Create Formal Public Procedure to Challenge Identifications

14. Unlike the statutory systems in place for challenging classified information and FOIA for non-sensitive information, there is currently no way to challenge CUI designations or identifications. To prevent CUI from entering a "black hole," the government should establish a procedure and precise guidelines for the public to challenge CUI identifications.

Incorporate Congressional Oversight in Designing the CUI Framework

15. To ensure there are adequate checks on the Executive Branch, Congress should pass legislation to define and regulate the CUI Framework. The legislative process should produce explicit instructions and expectations for when and how information should be identified as CUI, and the legislation should be designed to minimize the scope and amount of information included as CUI. The statutory regime also should specify how and when documents should be de-controlled and CUI markings removed from information. The current system designed for classified information is a good model for procedures to determine when CUI markings should be removed.

Monitor, Audit and Report on the CUI Process

16. In order to ensure CUI identifications are being made properly, audits should be conducted by the IGs of each federal agency that maintains documents with CUI markings. IGs should conduct random review on a periodic basis of CUI documents from each component of each Department which uses CUI designations. The IGs should assess whether applicable CUI policies, procedures, rules and regulations have been followed. They should describe any problems with the administration of applicable CUI policies, procedures, rules and regulations, including specific non-compliance issues and, as appropriate, recommend improvements in awareness and training. Each IG should annually report to the President, the Congress, and the public on his or her findings.

17. The National Archives and Records Administration (NARA) should publish an annual report to the President and Congress in which it quantifies the number of CUI control and de-control decisions, the number and position of individuals with authority to identify material, and the type of information that is being controlled. Such reports will enable the Executive Branch and Congress to monitor the costs and benefits of the system and to identify trends that may suggest the need to reform the system.

Explicitly Provide for Congressional and Court Access to CUI

18. Accountability requires checks and balances by the legislative and judicial branches. No control labels should justify withholding information from Congress and the courts. The CUI Framework therefore should explicitly provide that Congress and the courts may have access to CUI, and it should acknowledge that Congress and the courts will play a role in oversight of the CUI Framework.

Members of the Constitution Project's Liberty and Security Committee Endorsing "Reining in Excessive Secrecy: Recommendations for Reform of the Classification and Controlled Unclassified Information Systems" *

CO-CHAIRS

David Cole, Professor, Georgetown University Law Center

David Keene, Chairman, American Conservative Union

MEMBERS

Stephen E. Abraham (LTC, USAR (Ret.)), Partner, Fink & Abraham LLP; Lieutenant Colonel, Military Intelligence, United States Army Reserve (Ret)

Bob Barr, Former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy, American Conservative Union; Chairman, Patriots to Restore Checks and Balances; Practicing attorney

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

John W. Dean, White House Counsel, Nixon Administration

Mickey Edwards, Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton University; former Member of Congress (R-OK) and Chairman of the House Republican Policy Committee

Thomas B. Evans, Jr., Chairman, The Evans Group, Ltd.; Founder, Florida Coalition for Preservation; former Member of Congress (R-DE)

Eugene R. Fidell, Florence Rogatz Visiting Lecturer in Law, Yale Law School

Louis Fisher, Specialist in Constitutional Law, Law Library, Library of Congress

Michael German, Policy Counsel, American Civil Liberties Union; Adjunct Professor, National Defense University School for National Security Executive Education; Special Agent, Federal Bureau of Investigation, 1988-2004

Morton H. Halperin, Senior Advisor, Open Society Policy Center; Director of Policy Planning Staff, Department of State, Clinton Administration

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; former Undersecretary, Department of Homeland Security; former Administrator, Drug Enforcement Administration; former Member of Congress (R-AR); former United States Attorney, Western District of Arkansas

David Kay, Senior Fellow, Potomac Institute for Policy Studies; former Head, Iraq Study Group; former Special Adviser on the Search for Iraqi Weapons of Mass Destruction to the Director of the Central Intelligence Agency

David Lawrence, Jr., President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Thomas R. Pickering, Undersecretary of State for Political Affairs, 1997-2000; United States Ambassador and Representative to the United Nations, 1989-1992

Jack N. Rakove, W.R. Professor of History and American Studies and Professor of Political Science, Stanford University

L. Michael Seidman, Carmack Waterhouse Professor of Constitutional Law, Georgetown University Law Center

Earl Silbert, Partner, DLA Piper; United States Attorney, District of Columbia, 1974-1979; former Watergate Prosecutor

Neal Sonnett, Chair, American Bar Association Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism; former President, National Association of Criminal Defense Lawyers; former Assistant United States Attorney for the Southern District of Florida

Geoffrey R. Stone, Harry Kalven, Jr. Distinguished Service Professor of Law, the University of Chicago Law School

James A. Thurber, Director and Distinguished Professor, Center for Congressional and Presidential Studies, American University

Charles Tiefer, General Counsel (Acting), 1993-94 and Solicitor and Deputy General Counsel, 1984-95, U.S. House of Representatives

Don Wallace, **Jr.**, Professor, Georgetown University Law Center; Chairman, International Law Institute

John W. Whitehead, President, the Rutherford Institute

Lawrence B. Wilkerson (USA, Ret.), Visiting Pamela C. Harriman Professor of Government, College of William and Mary; Professional Lecture in the University Honors Program, George Washington University; former Chief of Staff to Secretary of State Colin Powell; Colonel, United States Army (Ret.)

Roger Wilkins, Clarence J. Robinson Professor of History and American Culture, George Mason University; Director of U. S. Community Relations Service, Johnson Administration

---

REPORTERS:

David Medine, WilmerHale

Anne Hazlett Sherwood, WilmerHale

CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel

---

[*] *Affiliations listed for identification purposes only.*