7-1-2011

Square Information, Round Categorization: Executive Order 13556 and Its Implementation Challenges

Austin Harris

STUDENT NOTE

Square Information, Round Categorization: Executive Order 13556 and Its Implementation Challenges

Austin Harris*

ABSTRACT

The Obama Administration is committed to establishing an unprecedented level of transparency and openness in order to garner the public's trust and ensure more effective government. Public access to government information is essential to a democracy, and the ability to share information across federal Executive Branch agencies is critical to the national security of the United States. In theory, President Obama's goal of increased openness and transparency in government is well served by the recently-signed Executive Order 13556, which calls for the standardization of Controlled Unclassified Information across the government. The goal of the new, standardized system is to make Controlled Unclassified Information easier to share across agencies and more accessible to the public. However, implementation of Executive Order 13556 faces significant challenges that will frustrate the goals of the Obama Administration, limiting public access and the sharing of Controlled Unclassified Information across the government until those challenges are addressed.

Compliance with Executive Order 13556 requires that existing Controlled Unclassified Information markings undergo a new review and designation process, placing existing designations into new, broader categories. This process requires intensive consideration by an examiner when attempting to place a particular piece of information into this small group of new categories to ensure maximum protection and shareability. The new review and designation process and the overall goals of Executive Order 13556 demand additional funding, personnel, and training in order to be effectively implemented. This is especially the case where some types of currently-existing Controlled Unclassified Information do not fit easily into the forthcoming new categorizations. Furthermore, local, state, tribal, and private sector partners, all of which have done business with the government through decades of "agency-centric"

* Juris Doctor candidate, University of Miami, May 2012. General Member of the U. MIAMI NAT'L SECURITY & ARMED CONFLICT L. REV.

information protection policies, will also need to adopt new practices to ensure adequate protection and compliance.

In addition, although Executive Order 13556's implementation will theoretically create a standardized system that will ensure information is not overprotected and is easily shareable, individual agencies with different missions and individual security professionals concerned with issues such as the "Mosaic Theory" will continue to default to increased protection. As a result, the public availability of Controlled Unclassified Information and its sharing among governmental agencies will be further limited by existing individual agency culture, the need to retrain personnel to focus on information sharing, and the abandonment of deeply-routed agency practices of overprotection.

Given the ever-growing challenge to national security, protecting information will be critical as the missions of agencies continue to expand in scope. Public access to and trust in its government are the cornerstones of a democracy, and balancing security interests with the free flow of information will be a great challenge for the United States in the coming decades. While Executive Order 13556 attempts to address this challenge, the federal government must correct existing problems to Controlled Unclassified Information access if Executive Order 13556's goals are to be successfully realized across the government.

TABLE OF CONTENTS

I. INTRODUCTION

The availability of, and access to, information across the government is paramount to the national security of the United States and is essential to the function of a democratic society.[1] The Obama Administration is committed to establishing an unprecedented level of transparency and openness in order to garner the public's trust and ensure a more effective government.[2] This change is in stark contrast to the George W. Bush Administration, which is characterized as one among the most secretive in history.[3] Striking a balance between the need for public access to government information and protecting sensitive information from unauthorized dissemination is essential to the national security and democratic governance of the United States.[4] At the same time, modern threats require the ability of the Executive Branch agencies to share information with one another while ensuring the protection of sensitive information needed to carry out their mission of safeguarding the national security of the United States.[5]

Concerned citizens or organizations in a democracy will request government information to keep a watchful eye on how their sovereign is behaving or to advance their own interests.[6] However, an outside observer may

---

[1] *E.g.,* Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 399 (2009).

[2] Transparency and Open Government, 74 Fed. Reg. 4,685 (Jan. 26, 2009).

[3] Patrice McDermott, *Withhold and Control: Information in the Bush Administration*, 12 KAN. J.L. & PUB. POL'Y 671, 671 (2003).

[4] *See* Stephen J. Schulhofer, *Secrecy and Democracy: Who Controls Information in the National Security State?* 3–4 (N. Y. Univ. Pub. Law and Legal Theory at NELLCO Legal Scholarship Repository, Working Paper No. 217, 2010) (describing congressional access and broad public disclosure as "crucial for prudent national security policy"), *available at* http://lsr.nellco.org/nyu_plltwp/217/; Devin Fensterheim, *He Who Protects Everything Protects Nothing: Secrecy and Democratic National Security*, WORLD AFF. REV. Apr. 2006, at 21, 21–22 (2006) (discussing the inherent conflict between government transparency and the need for security in certain information).

[5] *See* Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 279–81 (2010) (discussing information sharing as a counterterrorism initiative "virtually everyone supports" and the efforts by Congress and the Executive Branch to promote information sharing across the government).

[6] *See* Aftergood, *supra* note 1, at 399 (discussing the free flow of information to interested members of the public as a prerequisite to their ability to hold elected officials accountable); James O'Reilly, *FOIA and Fighting Terror: The Elusive Nexus Between Public Access and Terrorist Attack*, 64 LA. L. REV. 809, 810 (2004) (listing the various classes of people and organizations who submit Freedom of Information requests).

not be clear as to the need for information sharing across the government, or, on the other hand, may not be certain why an agency would not be inclined to share its information with other government agencies. The same observer will also wonder why a democratic government would not be willing to share information with its citizens that does not meet a sensitivity level to qualify it for classified status. For purposes of this article, consider the following two hypotheticals while assuming that neither piece of requested information qualifies as classified material.

"Hypothetical One": Prior to September 11, 2001, an agency concerned about the Oklahoma City Bombing wants to mitigate any damage its headquarters could sustain in an attack carried out in a similar manner. The agency devises a list of federal buildings that it believes possess the most secure design and damage-mitigating features. The agency believes that, of all the buildings listed, the Pentagon will have the best information available, but, oddly enough, the Pentagon refuses to share particular information about its most recent bomb-proofing projects.

"Hypothetical Two": A citizen is performing research on the military installation near his home. He knows that there are munitions and ordnance stores around the area and, concerned for the safety of his community, wants to know the damage that could be done if a store were to detonate. He files the proper paperwork to gain access to the information, but the military base refuses to release the information to him.

The two hypotheticals have foundations in real world events.[7] The section of the Pentagon that sustained damage during the 9/11 Terrorist Attacks, Wedge One, had been retrofitted as early as 1998 with heavy-duty, blast-resistant windows designed to minimize damage from an explosive attack.[8] In addition, a report detailing the bomb-proofing features of the Mark Center, a building in Alexandria, Virginia, soon to house 6,400 Department of Defense ("DoD") personnel, was found available on a public government internet

[7] *See* Milner v. Dep't of the Navy, 131 S. Ct. 1259 (2011); *Greening of the Pentagon*, U.S. ENVTL. PROT. AGENCY, http://www.epa.gov/epp/pubs/case/penren.htm (last updated May 12, 2010).

[8] *See* U.S. ENVTL. PROT. AGENCY, *supra* note 7 ("The first renovation efforts in the section called "Wedge 1" included blast-resistant windows . . . [B]ecause of the blast-resistant windows and other force protection measures, although horrific destruction was endured in the Wedge 1 area, studies have shown that the newly renovated and reinforced materials in Wedge 1 lessened the potential for greater destruction.").

website.[9] The pages of the report were marked "For Official Use Only," and the posting was described as a "recipe for attack."[10]

The concerned citizen in Hypothetical Two is similar to the citizen in *Milner v. U.S. Dep't of the Navy.*[11] *Milner* was focused on a Freedom of Information Act[12] ("FOIA") request[13] where Mr. Milner sought copies of the maps depicting the blast radius of a potential explosion of the munitions and ordnance stores around his community.[14] The concerned citizen in Hypothetical Two may submit a FOIA request in attempt to acquire the desired information, and the Department of the Navy may be replaced by any agency holding the information subject in the FOIA request. The Department of the Navy refused to release the maps to Mr. Milner, believing that their dissemination would threaten the security of the base and the surrounding community. The United States Supreme Court, although rejecting the Department of the Navy's initial FOIA-based reasoning for the withholding, remanded the case and pointed out that other FOIA exemptions still existed.[15]

The information sought in both hypothetical scenarios was withheld on the basis of its Controlled Unclassified Information ("CUI") designation. The reasoning for the designation (and withholding) may be based on concerns for an unauthorized dissemination, which could provide an enemy of the United

---

[9] Mark Hosenball & Missy Ryan, *Anti-bomb Plan for Pentagon Annex Posted Online*, REUTERS, Apr. 19, 2011, http://www.reuters.com/article/2011/04/19/us-usa-pentagon-security-exclusive-idUSTRE73I6KK20110419.

[10] *Id.*

[11] *Milner*, 131 S. Ct. 1259 (2011).

[12] Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2006).

[13] *See Milner*, 131 S. Ct. at 1262.

[14] *Id.* at 1263 ("To aid in the storage and transport of these munitions, the Navy uses data known as Explosive Safety Quantity Distance (ESQD) information. ESQD information prescribes "minimum separation distances" for explosives and helps the Navy design and construct storage facilities to prevent chain reactions in case of detonation. The ESQD calculations are often incorporated into specialized maps depicting the effects of hypothetical explosions." (internal citations omitted).

[15] *Id.* at 1271 ("Exemption 3 also may mitigate the Government's security concerns. That provision applies to records that any other statute exempts from disclosure, thus offering Congress an established, streamlined method to authorize the withholding of specific records that FOIA would not otherwise protect. And Exemption 7, as already noted, protects "information compiled for law enforcement purposes" that meets one of six criteria, including if its release "could reasonably be expected to endanger the life or physical safety of any individual." The Navy argued below that the ESQD data and maps fall within Exemption 7(F), and that claim remains open for the Ninth Circuit to address on remand.") (internal citations omitted).

States access to material for part of a larger plan.[16] Other pieces of CUI information, such as those related to law enforcement investigations, are withheld to prevent suspects from escaping capture or surveillance.[17] Furthermore, an agency may choose to withhold information from release in order to protect an intelligence source and ensure its safety and anonymity.[18]

This article concerns the Obama Administration's attempt to streamline the categorization process for CUI, Executive Order 13556 ("EO 13556").[19] Specifically, the article's focus is on the duties outlined by EO 13556 and the challenges to its effective implementation. CUI is defined as:

> [A] categorical designation that refers to unclassified information that does not meet the standards for 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 policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.[20]

Through EO 13556, the Obama Administration hopes to improve access to CUI for both the public and among Executive Branch agencies, thereby increasing transparency and ensuring information needed by agencies to execute their missions is shared across the government.[21] Successful implementation of EO 13556 would, in theory, remove the information sharing and government

---

[16] This idea is known as the "Mosaic Theory." It is discussed in detail in the section entitled, "*The 'Mosaic Theory*.'"

[17] Michael P. Goodwin, *A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts*, 32 HASTINGS COMM. & ENT. L.J. 179, 185 (2010) ("[T]here is little question that the effective conduct of foreign and military affairs requires a certain degree of secrecy . . . . In some cases this is easy, such as when public disclosure would alert the target of an investigation of the government's interest in him.").

[18] Sales, *supra* note 5, at 283–84.

[19] Exec. Order No. 13,556, 75 Fed. Reg. 68,675 (Nov. 9, 2010) [hereinafter EO 13,556].

[20] Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673, para. 3(a) (May 9, 2008) [hereinafter Bush CUI Memorandum]. This memorandum has since been rescinded by Executive Order 13,556. EO 13,556, *supra* note 19, § 6(g). The CUI Task Force recommended in its report that the definition of CUI be simplified to "all unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls." PRESIDENTIAL TASK FORCE ON CONTROLLED UNCLASSIFIED INFO., REPORT AND RECOMMENDATIONS 11 (2009). [hereinafter CUI TASK FORCE REPORT].

[21] *See* EO 13,556, *supra* note 19, § 1.

transparency issues, such as those raised by Hypotheticals One and Two, unless there is a compelling need to protect the information from dissemination.

Part II of this paper is focused on examining and discussing EO 13556 and CUI generally. Part III traces the history of CUI information and describes the major recent events leading to EO 13556. Understanding the historical context of the evolution of EO 13556 is essential to the examination of its importance to the national security of the United States. Part IV is concerned with detailing the duties and other provisions of EO 13556. Next, Part V examines the challenges of implementation that the government and affected parties must address to effectively carry out EO 13556's directives and goals.[22] Recommendations follow in Part VI; their purpose is to provide ideas, which could ease the challenges and reduce the cost of implementation. Finally, Part VII concludes that EO 13556, while excellent in theory, is likely to face many challenges if it is to be effectively implemented. Overcoming those challenges requires changes to the existing information sharing system and the granting of stronger authority, larger staff, and more funding to the Executive Agent ("EA") to ensure an optimum environment for openness with security.

II. EO 13556 AND CUI

Currently, executive departments and agencies have employed an "inefficient, confusing patchwork" of safeguards and categorizations concerning information that is not classified[23] but still requires protection or dissemination controls, also known as CUI.[24] The type of information traditionally falling under this categorization usually concern privacy, security, proprietary business interests, and law enforcement investigations.[25] Examples include a myriad of items, ranging from investigations of individuals with possible terrorist ties, to business information related to the development of military hardware, to the personal information of agency employees.[26] To gauge the extent of CUI across the Executive Branch, President Obama issued a memorandum directing department and agency heads to, among other things, "ensur[e] that the

---

[22] While effective public access is an important part of the CUI discussion, this paper focuses primarily on intergovernmental and agency-specific issues and practices that must be addressed to ensure implementation of EO 13556. Public access will be discussed as a means of illustration within the paper.

[23] The levels of *classified* information in ascending order of potential damage to national security are "confidential," "secret," and "top secret." Exec. Order No. 12,958, 60 Fed. Reg. 19,823, at 19,826 (Apr. 20, 1995), *reprinted as amended by* Exec. Order 13,292, 68 Fed. Reg. 15,315 (Mar. 28, 2003).

[24] EO 13,556, *supra* note 19, § 1.

[25] *Id.*

[26] CUI TASK FORCE REPORT, *supra* note 20, at 33–34; *Cf.* EO 13,556, *supra* note 19, § 1. See Hypotheticals One and Two for additional examples.

handling and dissemination of information is not restricted unless there is a compelling need[,]"[27] and to report their findings. In order to accommodate this directive, the leadership of several executive agencies led a collaborative effort[28] to seek out information currently listed as Sensitive But Unclassified ("SBU").[29] The agencies issued recommendations as to how the information could be reassessed, and consequently, more easily accessed by the public or other agencies.[30]

On November 4, 2010, President Obama signed EO 13556.[31] EO 13556 establishes "an open and uniform program for managing information that requires safeguarding[32] or dissemination controls[33] pursuant to, and consistent with, law, regulations, and Government-wide policies . . . ."[34] Among all of the executive departments and their agencies, over 100[35] different categorizations

---

[27] Memorandum on Classified Information and Controlled Unclassified Information, 2009 DAILY COMP. PRES. DOC. 408, § 2(b)(ii) (May 27, 2009) [herein after Obama CUI Memorandum].

[28] CUI TASK FORCE REPORT, *supra* note 20, at 2. The group assembling this report is referred to as both the "Interagency Task Force on Controlled Unclassified Information" and the "Presidential Task Force on Controlled Unclassified Information." This paper adopts the name, "CUI Task Force." Special credence should be afforded to this report as EO 13556 calls for consideration to be given to the report specifically. The agencies involved in the assembly of the CUI Task Force report were the Department of Justice, Department of Homeland Security, Department of Defense, Department of Health and Human Services, Department of State, Office of Management and Budget, Office of the Director of National Intelligence, Department of the Interior, Department of Agriculture, Federal Bureau of Investigation, National Archives and Records Administration, and the Program Manager of the Information Sharing Environment. *Id.*

[29] Most types of information meeting SBU categorization was redesignated as CUI. Bush CUI Memorandum, *supra* note 20, at para. 1.

[30] *See* CUI TASK FORCE REPORT, *supra* note 20.

[31] EO 13,556, *supra* note 19.

[32] "'Safeguarding' means measures and controls that are prescribed to protect controlled unclassified information." Bush CUI Memorandum, *supra* note 20, at para. 3(j). "'Safeguarding' means measures and controls to protect CUI from unauthorized access resulting from theft, trespass, or carelessness." CUI TASK FORCE REPORT, *supra* note 20, at 8.

[33] "Dissemination controls are instructions governing the extent to which dissemination is permitted or limited." CUI TASK FORCE REPORT, *supra* note 20, at 8.

[34] EO 13,556, *supra* note 19, § 1.

[35] Some of the markings used by agencies identifying CUI include "Sensitive," "Do Not Disseminate," "Eyes Only," "Limited Rights," "For Official Use Only," "Research and Development Agreement Information," "Limited Official Use – Law Enforcement Sensitive," "Personally Identifiable Information – Privacy Act of 1974," and "For Internal Use Only." CUI TASK FORCE REPORT, *supra* note 20, at 33–34.

exist for Controlled Unclassified Information ("CUI"),[36] and many of these ad-hoc, agency-specific policies have "led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing."[37]

Challenges to the access of information exist on many levels, and the inability to transmit information across government entities has been identified as one of the major causes in the failure to prevent the 9/11 Terrorist Attacks.[38] The 9/11 Commission recognized that the United States Government has access to an immense amount of information but has a "weak system for processing and using what it has."[39] Recognizing this problem, the 9/11 Commission opined, "The system of 'need to know' should be replaced by a system of 'need to share.'"[40]

Within the structure of sensitive government information exist two categorizations of information—classified information, denoted within the government by specific markings,[41] and CUI. Both types of information require varying levels of safeguarding and dissemination controls according to their sensitivity level. The need for protection of classified information is obvious due to its sensitive nature and the probability that its dissemination could cause harm to the United States Government, its personnel, or its missions. However, information categorized as CUI also requires protection, but its need for safeguarding is not as apparent. The general examples of CUI—privacy, security, proprietary business, and law enforcement investigations—are all types of information that need protection from unauthorized access or dissemination.[42] Furthermore, while some markings do not necessitate a clear need for protection, some of the currently-existing, agency-specific markings do.[43] These include: attorney client, IT [Information Technology] security-related, trade secret, bomb tech sensitive, controlled nuclear information, chemical-terrorism vulnerability information, and protected critical infrastructure information.[44]

---

[36] *Id.* at 5.

[37] EO 13,556, *supra* note 19, at 68,675.

[38] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U. S., *FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: EXECUTIVE SUMMARY* (2004) [hereinafter 9/11 COMMISSION REPORT EXECUTIVE SUMMARY] (describing how information could have been shared to disrupt attack plans and the call for a new focus on information sharing across the government); Schulhofer, *supra* note 4, at 53.

[39] 9/11 COMMISSION REPORT EXECUTIVE SUMMARY, *supra* note 38, at 24.

[40] *Id.*

[41] See *supra* text accompanying note 23.

[42] EO 13,556, *supra* note 19, § 1.

[43] CUI TASK FORCE REPORT, *supra* note 20, at 33–34.

[44] *Id.*

EO 13556 is primarily concerned with remedying the problems of inconsistent marking and safeguarding of CUI, unclear or unnecessarily restrictive dissemination policies, the problem of information sharing across the executive departments and agencies, and the lack of public transparency in the agency-specific CUI policies.[45] Correcting these problems will bolster national security through more effective information sharing among Executive Branch agencies that may require CUI obtained from other agencies to accomplish their missions. The Obama Administration's employment of EO 13556 will serve the goals of transparency and openness well in theory, but implementation will likely encounter obstacles associated with the practical application of EO 13556, both within and outside of the Executive Branch.

Writing on CUI presents unique challenges given the sensitive nature of the subject. While a substantial level of difficulty is to be expected when petitioning the government and its employees for information relating to classified information, EO 13556 has indeed proven to be a challenging subject on which to collect substantial "inside" information. Government officials will only speak to this issue under strict non-attributable status.[46] Despite these challenges, the extensive body of research relating to government information and its dissemination allows for realistic recommendations to ensure effective implementation of EO 13556.

III. HISTORICAL BACKGROUND

The need for secrecy in government actions can be traced back to the Revolutionary War.[47] George Washington and his officers in the Continental Army marked critical strategic documents requiring protection as "Secret" and "Confidential."[48] The first systematic procedures for protecting documents concerning "national defense" were created by War Department General Orders No. 3 in February 1912.[49] However, the current system for classified documents can be traced to Executive Order 8381 issued by President Franklin Roosevelt in March 1940, and in February 1950, President Truman issued Executive Order 10104, creating the classified markings in existence today.[50]

---

[45] EO 13,556, *supra* note 19, § 1.

[46] Given the ramifications of discussing a federal employee's opinions on the current administration's efforts; that is, an employee may consider that expressing negative comments or doubts would be career limiting.

[47] Harold C. Relyea, CONG. RESEARCH SERV. RL 33494, SECURITY CLASSIFIED AND CONTROLLED INFORMATION: HISTORY, STATUS, AND EMERGING MANAGEMENT ISSUES 1 (2008).

[48] *Id.*

[49] *Id.* at 2.

[50] *Id.*

In September 1951, Executive Order 10290 expanded the power of the president to create secrecy policy; classified information in the interest of "national security"; conveyed more latitude for the creation of secrets; and granted classification authority to nonmilitary, Executive Branch entities serving a role in "national security" policy.[51] These sweeping changes, however, suffered from extensive criticism from the press and the public, prompting President Eisenhower to issue Executive Order 10501 in November 1953, significantly changing the powers granted under Executive Order 10290.[52] For the next thirty years, Executive Order 10501 would serve as United States policy on classification procedures.[53] During these three decades, new Executive Orders continued to build on these reforms until President Reagan reversed this pattern in 1982 with Executive Order 12356.[54] In April 1995, the Clinton Administration issued Executive Order 12958, returning to the trend of reform instituted by the Eisenhower Administration; this Order was later amended by President George W. Bush with Executive Order 13292 in March 2003.[55]

The first references to SBU emerged in the 1970s.[56] In 1977, President Carter signed a Presidential Directive on Telecommunications Protection Policy[57] which mandated protection of unclassified, but sensitive communications "that could be useful to an adversary."[58] Several years later, National Security Decision Directive 145 ("NSDD–145")[59] instructed that "sensitive, but unclassified" information, the loss of which could negatively affect national security interests, should be "protected in proportion to the threat of exploitation and the associated potential damage to the national security."[60] NSDD–145 also alluded to the belief that pieces of unclassified information, taken in the aggregate, could reveal classified or other sensitive data and

---

[51] *Id.* at 3.
[52] *Id.*
[53] *Id.*
[54] *Id.* at 3–4.
[55] *See id.* at 4 (detailing the changes by Presidents Clinton and George W. Bush).
[56] *See* Genevieve J. Knezo, CONG. RESEARCH SERV. RL 31845, "SENSITIVE BUT UNCLASSIFIED" AND OTHER FEDERAL SECURITY CONTROLS ON SCIENTIFIC AND TECHNICAL INFORMATION: HISTORY AND CURRENT CONTROVERSY 11 (2004) *available at* http://www.fas.org/sgp/crs/RL31845.pdf; OMB WATCH, CONTROLLED UNCLASSIFIED INFORMATION: RECOMMENDATIONS FOR INFORMATION CONTROL REFORM 3 (2009) [hereinafter OMB WATCH, CUI REFORM].
[57] Presidential Directive on Telecommunications Protection Policy (PD/NSC–24), (Nov. 16 1977), http://www.jimmycarterlibrary.gov/documents/pddirectives/pd24.pdf.
[58] *Id.* ¶ 2(b).
[59] National Security Decision Directive 145 (NSDD–145) on National Policy on Telecommunications and Automated Information Systems Security (Sept. 17, 1984), http://www.fas.org/irp/offdocs/nsdd145.htm.
[60] *Id.* ¶ 2(b).

adversely affect national security.[61] NSDD–145 did not define the term "sensitive, but unclassified."

On October 29, 1986, President Reagan's National Security Advisor, John Poindexter, issued National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems ("NTISSP No. 2")[62] broadening the rationale for safeguarding "sensitive, but unclassified" information to "other government interests."[63] "Sensitive, but unclassified" was defined as "information the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests."[64] However, widespread criticism about the scope of NTISSP No. 2 and the powers it granted to the intelligence community led to the withdrawal of NTISSP No. 2 and usage of its definition for "sensitive, but unclassified."[65]

Shortly thereafter, the Computer Security Act of 1987[66] granted the National Bureau of Standards, since renamed the National Institute of Standards and Technology ("NIST"), the authority to enhance government-wide computer security standards and guidelines.[67] The Computer Security Act of 1987 defined the term "sensitive" as:

> [A]ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.[68]

---

[61] *Id.* intro., para. 2. This idea is now called the "Mosaic Theory."

[62] John M. Poindexter, National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems (NTISSP No. 2) (Oct. 29, 1986), http://www.fas.org/ota/reports/8706.pdf.

[63] *Id.* § II (Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.").

[64] *Id.*

[65] Knezo, *supra* note 56, at 13.

[66] Computer Security Act of 1987, Pub. L. No. 100–235, 101 Stat. 1724 (1988).

[67] Computer Security Act of 1987, Pub. L. No. 100–235, § 2(b) 101 Stat. 1724, 1724 (1988).

[68] Computer Security Act of 1987, Pub. L. No. 100–235, § 3(d)(4), 101 Stat. 1724, 1727 (1988).

The Computer Security Act of 1987 also granted agencies the discretion to identify which information in their systems was sensitive, identify the risks of any release of sensitive information,[69] and placed the responsibly for protecting sensitive information on the agencies.[70] Five years later in 1992, NIST issued guidelines to agencies to ensure protection of sensitive information.[71] These guidelines stated that the interpretation of the Computer Security Act of 1987's definition of sensitive resided with the agencies and that a "risk-based approach" should be utilized by the "owners" of sensitive information to determine which protections to place on such information.[72]

Since 1987, various agencies have used the definition of "sensitive" provided by the Computer Security Act of 1987 to identify SBU information,[73] while others have expanded it in various ways.[74] Such expansions included information exempted from disclosure under FOIA and information deemed sensitive by an individual agency based on its particular activities.[75] The lack of a uniform definition of "sensitive but unclassified" eventually led to an equivalence within the Department of Defense between "sensitive," as defined in the Computer Security Act of 1987, and the term "sensitive but unclassified"[76] and ultimately led to the emergence of the multitude of markings in existence today.[77]

CUI sharing and safeguarding problems have existed for decades, but the 9/11 terrorist attacks were the catalyst for addressing and attempting to correct many of these problems.[78] In 2004, President Bush signed into law the Intelligence Reform and Terrorism Prevention Act ("IRTPA")[79] which called for the President to "issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form . . . ."[80] IRTPA also established the Information Sharing

---

[69] Computer Security Act of 1987, Pub. L. No. 100–235, §§ 6(a)–(b), 101 Stat. 1724, 1727 (1988).
[70] Knezo, *supra* note 56, at 14.
[71] *Id.*
[72] *Id.*
[73] *Id.* at 16.
[74] *Id.* at 38.
[75] *Id.*
[76] *Id.* at 22
[77] *See generally id.* at 16–23 (discussing the different definitions of SBU used across the Executive Branch agencies).
[78] CUI TASK FORCE REPORT, *supra* note 20, at 7.
[79] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638 (2004).
[80] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1016(d)(1), 118 Stat. 3638, 3666 (2004).

Environment ("ISE"), which initially only handled the sharing of terrorism-related information.[81] In addition, IRTPA also established the Information Sharing Council to assist the President with his new tasks.[82] Although its informational scope was limited to terrorism information, IRTPA's ISE implementation outline provided a foundation from which EO 13556 could base its goals and structure.[83]

On December 16, 2005, President George W. Bush, through a memorandum,[84] issued guidelines to aid in information sharing[85] as specified in section 1016(d) of IRTPA.[86] The guidelines issued in the memorandum, while meant only for terrorism-related SBU information,[87] would again be reflected in the goals of EO 13556. Specifically, Guideline Three called for the standardization of SBU procedures across the federal government.[88] Guideline Three instructed that the "Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI [Director of National Intelligence], shall submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information . . . ."[89] The following year, in October 2006, the SBU Coordinating Committee began development of a Guideline Three Report.[90] The Committee consulted with National Archives and Records Administration's ("NARA") Information Security Oversight Office ("ISOO") and other federal offices

---

[81] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1016(b)(1), 118 Stat. 3638, 3665 (2004).

[82] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, §§ 1016(g)(1)–(2), 118 Stat. 3638, 3668 (2004).

[83] *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1016(b)(2), 118 Stat. 3638, 3665 (2004) (listing the attributes of information sharing).

[84] Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment, 41 WEEKLY COMP. PRES. DOC. 1874 (Dec. 16, 2005).

[85] *See id.* at 1875–78. The guidelines outlined were as follows: (1) Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE; (2) Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector; (3) Standardize Procedures for Sensitive But Unclassified Information; (4) Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners; and (5) Protect the Information Privacy Rights and Other Legal Rights of Americans.

[86] *Id.* at 1873.

[87] *Id.*

[88] *Id.* at 1877.

[89] *Id.*

[90] *CUI Chronology*, NAT'L ARCHIVES AND RECORDS ADMIN., http://www.archives.gov/cui/chronology.html (last visited Apr. 27, 2011).

alongside state, local, tribal, and private sector partners during the development of the Guideline Three Report.[91]

Seven months later, on May 7, 2008, President Bush signed a new memorandum ("Bush CUI Memorandum") that adopted CUI as the single designator for all SBU information within the ISE.[92] It also established the CUI Framework[93] for designating, marking, safeguarding, and disseminating CUI terrorism-related information. Further, it selected NARA as the EA, giving it the power and responsibility to oversee and ensure the implementation of the memorandum's directives.[94] NARA's dedication to information and document preservation and objectivity made it an ideal candidate for the new responsibilities.[95] Three distinct categorizations of CUI were established by the Bush CUI Memorandum: Controlled with Standard Dissemination,[96] Controlled with Specific Dissemination,[97] and Controlled Enhanced with Specific Dissemination.[98]

Furthermore, the Bush CUI Memorandum established the CUI Council as the primary general advisor to NARA on issues relating to the CUI Framework.[99] The CUI Council also assisted in developing the procedures, guidelines, and standards necessary to implement and maintain the goals of the new CUI Framework.[100] In addition, it ensured coordination among the departments and

---

[91] *Id.*

[92] Bush CUI Memorandum, s*upra* note 20, at para. 2(b) ("A uniform and more standardized governmentwide framework for what has previously been known as SBU information is essential for the ISE to succeed.").

[93] "CUI Framework" refers to the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of CUI terrorism-related information that originates in departments and agencies, regardless of the medium used for the display, storage, or transmittal of such information. *Id.* at para. 3(c).

[94] *Id.* at para. 21.

[95] OMB WATCH, CUI REFORM, *supra* note 56, at 6.

[96] Bush CUI Memorandum, s*upra* note 20, at para. 7(b)(i) ("[T]he information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.").

[97] *Id.* at para. 7(b)(ii) ("[T]he information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.").

[98] *Id.* at para. 7(b)(iii) ("[T]he information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.").

[99] *Id.* at para. 23(a).

[100] *Id.* at para. 23(b).

agencies participating in the CUI Framework.[101] Exceptions to information that could be categorized as CUI were also enumerated.[102] Concurrent with the Bush CUI Memorandum, the Archivist of the United States established the CUI Office within NARA to carry out the newly-established responsibilities.[103]

President Barack Obama, in his May 27, 2009, Presidential Memorandum on "Classified Information and Controlled Unclassified Information" ("Obama CUI Memorandum"), called for agencies to consider new measures, in addition to those listed in the Bush CUI Memorandum, "to further and expedite agencies' implementation of appropriate frameworks for standardized treatment of SBU information and information sharing."[104] To aid in this process, the Obama CUI Memorandum established the Presidential Task Force on Controlled Unclassified Information ("CUI Task Force"), which was given ninety days to assemble and submit to President Obama its recommendations on how the Executive Branch should proceed with respect to the CUI Framework and the ISE.[105] The CUI Task Force released its report in August 2009.[106] On November 4, 2010, President Obama issued Executive Order 13556, incorporating key elements of the CUI Task Force Report and broadening the scope of CUI to include *all* SBU information within the Executive Branch.[107]

IV. DUTIES UNDER EO 13556

Part of the focus of this article is the challenges facing by the federal government and its partners that currently hinder an effective, economically sound implementation of EO 13556. Therefore, it is critical to understand the requirements that EO 13556 places against the affected executive agencies, NARA as the EA, and the private and other governmental partners working with the federal government.

A. Departmental/Agency Duties

Effective implementation of EO 13556 begins with the heads of the agencies within the Executive Branch.[108] The agency heads provide the first level of analysis to determine the development of the new, standardized CUI

---

[101] *Id.* at para. 23(c).
[102] *Id.* paras. 27(a)–(d).
[103] NAT'L ARCHIVES AND RECORDS ADMIN., MEMORANDUM ON THE ESTABLISHMENT OF THE CONTROLLED UNCLASSIFIED INFORMATION OFFICE 1 (2008).
[104] Obama CUI Memorandum, *supra* note 27, § 2(a).
[105] *Id.* §§ 2(b)(i)–(iii).
[106] CUI TASK FORCE REPORT, *supra* note 20, at v.
[107] *See* EO 13,556, *supra* note 19, § 2(a).
[108] *Id*. § 3.

categories.[109] The head of every executive agency must review all of the categories and markings[110] used by the agency to denote CUI.[111] These various markings and categorizations include information that needs to be safeguarded as well as that which requires dissemination controls.[112] Upon reviewing the markings and categorizations, each agency head must submit to NARA a catalog of the proposed categories and their associated markings to be used within the agency.[113] Each category and subcategory must then be defined, along with its basis in law, regulation, policy for safeguarding or need for dissemination control.[114] The agency heads must accomplish these duties within 180 days[115] of the signing of EO 13556 and must later submit to NARA a "proposed plan for compliance with the requirements of this order, including the establishment of interim target dates."[116]

B. National Archives and Records Administration

NARA has the duty of ensuring the goals of EO 13556 are properly implemented.[117] Once the executive agencies submit their proposed CUI categories and markings and are consulted by NARA, the CUI Office must approve, in a timely manner, the new CUI categorizations that will be uniformly applied throughout the Executive Branch.[118] This approval lays the groundwork for all future categorization; in theory, agencies and the public should immediately know how accessible a piece of CUI is based on its categorization without having to worry about agency-specific markings and/or dissemination rules. In addition, the CUI Office has the authority under EO 13556 to develop and issue directives necessary for its implementation, and EO 13556 calls on NARA to consider the suggestions outlined by the CUI Task Force Report.[119] These suggestions, such as establishing a marking's "life cycle"[120] or providing incentives for the proper handling of CUI, help NARA identify the concerns of the

---

[109] *See id.*
[110] See CUI TASK FORCE REPORT, *supra* note 20, at 33–34 for a list of markings currently in use.
[111] EO 13,556, *supra* note 19, § 3(a)(1).
[112] *Id.*
[113] *Id.* § 3(a)(2).
[114] *Id.*
[115] *Id.* § 3(a).
[116] *Id.* § 5(a).
[117] *Id.* § 2(c).
[118] *Id.* § 4(a).
[119] *Id.* § 4(b).
[120] *See* CUI TASK FORCE REPORT, *supra* note 20, at 20–21 (describing "life cycle" as the length of time that a piece of CUI receives safeguarding and dissemination controls outlined in the CUI Framework. The current default "life cycle" recommended by the CUI Task Force is ten years, subject to exceptions.)

affected agencies and allow for development of responsive directives. Consistent with the deadline imposed on the other executive agencies, NARA has 180 days to issue the initial directives for implementation of EO 13556.[121]

In addition to assuming the responsibilities of category approval and directive issuances, NARA is assigned several additional duties under EO 13556.[122] Convened and chaired by NARA, interagency meetings are to be held to review and discuss the program established by EO 13556.[123] Furthermore, a public CUI registry listing the authorized categories and markings, as well as the applicable safeguarding, dissemination, and decontrol procedures, is to be created within one year of the date of the signing of EO 13556.[124]

The interagency meetings will afford an opportunity for individual agencies to address implementation challenges and concerns they may have with the new standardization process. Hence, agencies like those found in Hypothetical One, can voice their concerns about CUI sharing and the possible consequences should certain pieces of CUI be leaked to those not authorized for access. The public registry to be created will allow both the public and agencies to understand the meaning of the new categorizations and how accessible a certain piece of CUI will be, given its marking. For example, the citizen seeking the blast maps in Hypothetical Two will know, based on the documents' CUI markings, how accessible to him the documents will be and whether a FOIA request likely will be worth his time. Further, the procedures for safeguarding, dissemination, and decontrol to be included in the registry will give agencies clear directive on how CUI is to be handled for both intergovernmental and public access purposes.[125]

NARA must also consult with representatives of state, local, and tribal partners, and with private sector representatives, on matters relating to its categorical approval and directive issuance responsibilities.[126] Such consultations provide government partners direct access to the EA as well as an opportunity to understand the new standardization and clarify the implementation duties to be undertaken. After all agencies' compliance plans have been reviewed and those agencies and the Office of Management and Budget have been consulted, NARA will establish deadlines for implementation of EO 13556's directives.[127] Finally, NARA has a regular reporting requirement to

---

[121] EO 13,556, *supra* note 19, § 4(b).
[122] *Id.* §§ 4–5.
[123] *Id.* § 4(c).
[124] *Id.* § 4(d).
[125] *See id.*
[126] *Id.* § 4(f).
[127] *Id.* § 5(b).

keep the Government updated on the implementation efforts of the affected agencies.[128]

C. Other Select Provisions

Aside from the duties specifically directed toward agencies and NARA, EO 13556 provides special individual authority to the DNI.[129] The DNI, after consulting with the heads of the affected agencies, may issue directives and guidelines necessary to implement EO 13556 with respect to intelligence and intelligence-related information.[130] This special provision provides another layer of oversight by allowing the DNI to implement extra procedures to ensure the most sensitive CUI is properly protected.

Furthermore, EO 13556 establishes a presumption of "non-CUI designation" when there is doubt about a particular piece of information's need for safeguarding or dissemination control.[131] That is, if there is a question of whether the level of sensitivity warrants a CUI categorization, that piece of information will default to a "normal," or non-CUI, non-classified status. Such status, in theory, affords a piece of information the ability to be disseminated to the public or shared among federal agencies without delay. A final and crucial provision addressing execution of EO 13556 provides that implementation shall only take place upon the availability of appropriations.[132]

V. CHALLENGES TO IMPLEMENTATION

Theoretically, EO 13556 will increase openness across the government, but the challenges in implementing EO 13556 will likely delay complete, successful realization of its goals for an indefinite amount of time. The parties affected by the implementation of EO 13556 will face staffing, training, and fiscal challenges while attempting to safeguard their sensitive information and carry out their missions.

---

[128] *Id.* § 5(c). ("In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.")

[129] *Id.* § 6(b).

[130] *Id.*

[131] *Id.* § 3(b).

[132] *Id.* § 6(e). As will be discussed in the remainder of the paper, funding for the undertaking of EO 13556's directives will likely pose a major challenge to its implementation.

A. Departmental/Agency Training and Personnel

Proper training is the first line of defense in protecting CUI. Every executive agency that handles CUI has its own management procedures and markings for the material, and its personnel have been trained in an agency-specific manner in the proper analysis, marking, and safeguarding of its information.[133] For example, the CUI Task Force identified many current categorizations specific to the DoD.[134] At the same time, it identified information specific to federal grand juries, as well as trade secrets and sensitive business information that needs to be protected.[135] Various combinations of these types of information can exist across any agency at a given time, and, depending on the levels of safeguarding appropriate to each agency-specific category, different treatment is required to assure the different categories of information are adequately protected.[136] Agencies' information management personnel will need to be trained in the use of the forthcoming new categories to ensure proper marking and continued protection of the information. The different types of CUI and the need for specific dissemination controls are illustrated in Hypotheticals One and Two.

To ensure that standardization is achieved, standardized training must be provided to all security professionals overseeing CUI categorization.[137] NARA must ensure that the new basic training is geared toward an information-sharing perspective and not hindered by individual agency-tailored training programs. Each agency will need to expend the appropriate amount of funding to secure proper training and, in the event that additional employees are needed to oversee the categorization process, more tax dollars must be expended to this end.[138] However, agencies are not free to work with an unlimited budget. The CUI Task Force first recognized the challenges to funding in its report to President Obama in August 2009, acknowledging that "Full implementation of the CUI Framework requires *significant resources* . . . ."[139]

---

[133] *See* CUI TASK FORCE REPORT, *supra* note 20, at 5.

[134] *Id.* at 33–34.

[135] *Id.*

[136] *Cf. id.* at 5–6 (discussing inconsistent SBU policies across agencies and a lack of clarity as to how those policies apply).

[137] *Id.* at 22 ("A dedicated, centralized training program is critical to [the training] effort.").

[138] *See* Info. Security Oversight Office, *2009 Cost Report* 3, (2010), http://www.archives.gov/isoo/reports/2009-cost-report.pdf. While this report addresses the costs of classifying information, without referencing CUI categorization costs, the costs of "Security Management, Oversight, and Planning" and "Classification Management," two categories closely related to CUI, have increased sharply and steadily, respectively.

[139] CUI TASK FORCE REPORT, *supra* note 20, at 25 (emphasis supplied).

EO 13556's goal of standardization of CUI is frustrated by the real-world fact that different agencies' missions and specific categories of CUI will in fact require customized training. Complicating factors in uniform training—and therefore, uniform implementation—are evident in the CUI Task Force Report:

> Each agency should be encouraged to create training that is tailored to its particular needs and mission. This is especially true in the ISE agencies, where the tension between sharing and protecting critical information is greatest. Training in this area requires a strong emphasis on the exercise of individual judgment in ensuring that the CUI Framework does not have a chilling effect on information sharing . . . The EA should establish a baseline training program sufficient to educate federal employees on the key principles underlying the CUI Framework . . . Intermediate and advanced level training should be developed by agencies, in consultation with the EA, to address increased requirements for expertise and sophistication in managing CUI.[140]

Another important aspect that is not addressed specifically within EO 13556 is that of retroactive recategorization. EO 13556 did not specify the responsibilities of agencies for marking pieces of information which already have an agency-specific categorization. In its recommendations to President Obama, the CUI Task Force addressed this issue and determined that material which was previously printed, disseminated, or otherwise categorized, should not be remarked and left the recategorization of material that continues to be disseminated to the discretion of the individual agency.[141] Neither EO 13556 nor the CUI Task Force Report details why such discretion is left to the agencies.

Given the federal government's desire to maintain relations with local, state, tribal, and private sector partners while ensuring CUI protection,[142] the CUI Task Force may have allowed agencies to retain individual discretion concerning the remarking of previously-categorized CUI in order to facilitate these partners' progressive transition into the new standardized CUI schema. However, this stymies the EO 13556's goal of standardization, as new categories will exist alongside the older markings still in use with various agencies. Agency and government partner personnel working with both sets of categories must then essentially perform a duty delineated to NARA: place the old information within the correct new category to ensure the appropriate level of protection and shareability. This problem can be mitigated with proper training of agency

---

[140] *Id.* at 22–23. The exercise of individual judgment will be addressed in the section *Entrenched Institutional Bias Against Information Sharing*.

[141] *Id.* at 26.

[142] *See* EO 13,556 *supra* note 19, § 4(f).

personnel by NARA, but this may not be the case where a governmental partner has not had the benefit of new training regarding the new marking schema.

The CUI Task Force has left determinations of employee incentives and sanctions to the discretion of the agencies.[143] They are directed to consider employee performance under the CUI Framework in promotion and award decisions and are guided to impose administrative sanctions for non-compliance with CUI, safeguarding, or dissemination control standards.[144] Remiss in this regard, EO 13556 neither addresses how federal employees should be evaluated nor outlines how sanctions should be imposed for violations. Any agency that is lax[145] in its enforcement sanctions or that does not consider CUI policy violations equally as seriously as other security violations hinders implementation of EO 13556 and frustrates the efforts of other agencies and their employees to properly carry out its directives.

B. National Archives and Records Administration

William J. Bosanko, director of NARA's CUI Office and former director of its ISOO, carries out the responsibilities of EO 13556, Executive Order 13526, and 12829, as amended.[146] Recognizing the vast categorizations of CUI, Bosanko and his office will shoulder the task of narrowing down the "wild, wild West"[147] of currently existing markings into a smaller, standardized group.

The challenge to NARA is to create a new schema that will ensure sharing across the government and with the public while affording the proper level of protection to every piece of CUI. Essentially, the CUI Office must take over 100 different markings and condense them into a few new categories that will cover all CUI across the government.[148] To help frame this problem, consider the CUI in Hypothetical One as fitting into "New Category X," but the CUI in Hypothetical Two does not fit well into New Category X and cannot be assigned to any other category. The problem with a "mal-fitting" piece of CUI is that an agency will be posed with either overprotecting, to ensure security, or underprotecting, to

---

[143] CUI TASK FORCE REPORT, *supra* note 20, at 23.

[144] *Id.*

[145] This should not be read to imply that an agency would act irresponsibly; rather, an agency is likely to inadvertently overlook a violation due to a lack of funding or adequately trained staff to ensure compliance with EO 13556.

[146] *Director, Information Security Oversight Office,* NAT'L ARCHIVES & RECORDS ADMIN., http://www.archives.gov/isoo/about/director.html (last visited May 8, 2011).

[147] Sean Reilly, *Executive Order Tightens Rule on "Controlled Unclassified" Info*, FEDERAL TIMES, Nov. 16, 2010, http://www.federaltimes.com/article/20101116/AGENCY03/11160302/.

[148] While there is no "magical" number of categories, creating too many categories recreates the original problem.

ensure shareability and wider dissemination. Because each agency currently marks such information in its own specific manner, NARA will have to create a marking applicable to multiple CUI designations across many agencies. NARA must design a system which can protect the CUI in both hypotheticals while ensuring its shareability with the public and across the government.

Given the sheer quantity of information and affected agencies,[149] the CUI Office will need to expand its operation and manpower if it is to successfully oversee the implementation of EO 13556.[150] In fact, the CUI Office only has ten full-time employees;[151] given the mammoth task EO 13556 assigns to NARA, more manpower will be required to achieve full, effective implementation. Bosanko is not confident that EO 13556 would reduce the amount of information designated as CUI.[152] Furthermore, Bosanko also recognizes that the modern structure for handling information in the federal sector has changed significantly,[153] and his office is now in charge of "potentially more data than exists in classified files."[154] As NARA works to publish a public registry to catalogue the new CUI categories,[155] Bosanko's office will be working with the various agencies across the Executive Branch to determine which documents need the protection of the CUI Framework.[156]

As the EA, NARA is the natural "go-to" source for categorization questions that an agency's information managers are unable to answer. Additionally, individual agencies will look to NARA to provide critical training to

---

[149] See Aftergood, *supra* note 1, at 401–02 (describing how classification—and overclassification—have increased in recent years and that in 2008, classification activity had increased to over 23 million classification actions per year). Although Aftergood is addressing *classified* information, parallels can be drawn with CUI, especially since some predict the volume of CUI surpasses that of classified information. A 1998 report for the Secretary of Defense and the Director of Central Intelligence estimated that upwards of three quarters of all government held information may be "sensitive but unclassified." JOINT SEC. COMM., REDEFINING SECURITY: A REPORT FOR THE SECRETARY OF DEFENSE AND THE DIRECTOR OF CENTRAL INTELLIGENCE ch. 2 (1998), *available at* http://www.fas.org/sgp/library/jsc/chap2.html.

[150] Reilly, *supra* note 147 (denoting that as of twelve days after EO 13556's signing, the ISOO has fewer than a dozen staff members handling CUI issues).

[151] E-mail from Carla Riner, Lead for Policy, Controlled Unclassified Info. Office, Nat'l Achieves & Records Admin., to author (Mar. 23, 2011, 15:30 EST) (on file with author).

[152] Reilly, *supra* note 147.

[153] *See* Max Cacas, *Executive Order Seeks to Simplify Document Classification*, FEDERAL NEWS RADIO, Nov. 10, 2010, http://www.federalnewsradio.com/?sid=2112686&nid=35 (describing how agencies have moved away from "memos and letters" which warranted an "agency-centric" approach).

[154] Reilly, *supra* note 147.

[155] EO 13,556, *supra* note 19, § 4(d).

[156] Cacas, *supra* note 153.

meet the new directives. The need for an expanded staff to provide sufficient expertise and manpower to oversee the implementation of EO 13556 will require more funding. The CUI Task Force, aware of this critical need because of the "extraordinary efforts"[157] required of the EA, made a point to denote the vital role the EA would serve and its need to be "appropriately resourced."[158] An approximate estimate of funding[159] and staffing[160] required for implementation remains elusive as no figures are available at this time. There is little doubt, however, that NARA, faced with the daunting task of successfully carrying out EO 13556, will need to expand to accomplish its duties.[161]

C. State, Local, Tribal, and Private Sector Partners

EO 13556 reaches out to entities beyond the federal government.[162] State, local, tribal, and private sector partners will be expected to assist in protecting CUI that the government has entrusted them to access (and to provide) in their capacity as partners of the federal government.[163] Like the executive agencies, many of these partners have been in business with the federal government for many years and have developed their own practices of marking and information dissemination.[164] Those that own or handle CUI that are subject to the new standardized marking system will need to revisit their policies and practices to ensure compliance under EO 13556 and all other applicable law.

---

[157] See the Hypothetical One and Two discussions at the beginning of Part IV.

[158] CUI TASK FORCE REPORT, *supra* note 20, at 27 ("The extraordinary efforts required of the EA to develop and implement the expanded scope CUI Framework, as well as the criticality of EA effectiveness in those efforts to the success of the CUI Framework, should be recognized and appropriately resourced to include funding, permanent staff, and agency detailees.").

[159] E-mail from Carla Riner, Lead for Policy, Controlled Unclassified Info. Office, Nat'l Achieves & Records Admin., to author (Feb. 25, 2011, 16:50 EST) (on file with author).

[160] *See* CUI Task Force Report, *supra* note 20, at 25–26.

[161] *Id.* at 26 ("The Task Force recognizes that should the recommendation to expand the scope of CUI be accepted, the EA would need to provide extraordinary support to non-ISE agencies to ensure effective implementation of the CUI Framework, and the EA's staffing and resource requirements would have to be addressed. Likewise, even with a phased implementation as recommended herein, successfully implementing the CUI Framework without impeding existing operations and programs would require that the agencies receive clear budgetary guidelines from OMB, and that the necessary resources be made available.").

[162] EO 13,556, *supra* note 19, § 4(f).

[163] *See id.* §§ 4(f), 6(a)(2).

[164] *See* O'Reilly, *supra* note 6, at 818 (describing local government employees as the "Achilles heel" of dissemination control).

These partners will be under the same strain as the executive agencies in training employees and in understanding how the CUI they handle should be categorized and to whom it may be disseminated. While the partners are being consulted by NARA, unlike the executive agencies,[165] they will not be able to submit their own categories, and these partners must adapt any former "partner-specific"[166] markings to match those the EA dictates. Furthermore, these partners may be caught in the confusion resulting from the marking initiation process; as agencies decide, at their discretion,[167] whether to apply new categorical markings to existing CUI, government partners must be ready to properly handle the newly-marked forms to assure their protection.

D. Entrenched Institutional Bias Against Information Sharing

The CUI Task Force's recommendation does not adequately address the fact that different agencies may have different ideas concerning the kind of information that needs to be safeguarded.[168] This can hinder sharing, based on the various types of information handled, the size of the agencies across the Executive Branch, and the various missions of the agencies.[169] Moreover, agencies must overcome their deeply-rooted "agency-centric"[170] historic practices and gear their information management style to an Executive Branch-wide sharing style.[171]

Part of the mission of agencies across the Executive Branch, especially those in the intelligence community, is to train and deploy agents specifically to gather information from sources and report that information back to their home

---

[165] EO 13,556, *supra* note 19, § 4(f).

[166] This term refers to markings invented by governmental partners designed to correspond to the safeguarding and dissemination protocols called for by the existing CUI categories. A contractor, for example, may employ a marking "Project/Government Sensitive" to tell employees that the information needs to be controlled and not accessible to those outside of the workplace. Examples of CUI found by the CUI Task Force for information which is accessible to partners and government likely includes the categories "Research and Development Agreement Information," "Confidential Business Information," "Trade Secret," "Contractor Access Restricted Information," and "Confidential Contract Proposal Information." CUI TASK FORCE REPORT, *supra* note 21, at 33–34.

[167] *Id*. at 26.

[168] *Cf. id.* at 14–16 (listing and describing how agencies should identify and mark CUI and establish CUI programs).

[169] Riner, *supra* note 159.

[170] *See* CUI TASK FORCE REPORT, *supra* note 20, at 33–34 (identifying some CUI markings as Department of Defense specific); *Cf.* Reilly, *supra* note 147 (discussing steps taken by different agencies and the DNI to comply with EO 13556).

[171] Riner, *supra* note 159.

offices for analysis.[172] CUI issues may arise when an agent, working on behalf of his agency, returns sensitive information back to his home office where, subsequently, there is disagreement among those at various levels of the organization concerning how the agent's original information should be categorized. Agencies generally default to protectionist practices when it comes to categorizing and sharing information,[173] a practice deeply rooted in decades-old, agency-specific policies[174] designed to protect the interests of the agencies and their missions. Indeed, sharing information has long been viewed as a "career stopper" for agents.[175] Information originating in or under the control of an employee's home agency, which is then shared and subsequently inadvertently disclosed or otherwise compromised due to the receiving agency's carelessness, can have severe negative consequences on that employee's career.[176]

In addition, problems arise in agency-specific circumstances where protecting a source is critical to ensuring that the source continues to supply the agency with information.[177] This area of contention regarding information sharing originates in an agency's culture, which can best be thought of as the inverse of Hypothetical Two. In this inverse hypothetical, a source from Country X is providing information—for example, the location of munitions stores—to an agency or a contact working on behalf of a specific agency. Having expended great amounts of time and funding seeking out and developing this source, the agency would naturally is loathe to risk compromising its source. Should news break in the United States or abroad of covert actions taking place in Country X, the source may "dry up." Agencies, therefore, are uneasy sharing information whose dissemination to the wrong individual could compromise the mission or, at worst, cause the death of sources providing intelligence to U.S. agents.

Finally, the history of SBU reveals instances where agencies have demonstrated a bias against information sharing.[178] For example, in 1992, NIST

---

[172] *See* Sales, *supra* note 5, at 304 (describing intelligence collection in "private-sector" terms).

[173] *See* Aftergood, *supra* note 1, at 403; *see also* Sales, *supra* note 5, at 281–83 (discussing why intelligence agencies are risk averse, tend not to share information, and their perceived threats to their own interests when sharing information).

[174] Riner, *supra* note 159.

[175] Sales, *supra* note 5, at 283.

[176] *Id.* at 325–28.

[177] *See id.* at 283–84 (emphasizing that intelligence agencies occasionally have compelling reasons not to share a particular pieces of information, especially where sharing might compromise a sensitive source or method of data collection).

[178] *See generally* Knezo, *supra* note 56, at 14–18 (describing various agencies' directives on what protection levels should be afforded to CUI, under what circumstances it should be released, and to whom it should be released).

emphasized that information "owners," not [government computer] system operators, should set the level of protection their information requires.[179] This agency-specific deference allows agencies to determine CUI protection classifications independent of other agencies, contributing to the growing number of individual agency CUI markings. Further bias against information sharing is demonstrated by DoD Regulation 5200.1,[180] which limits dissemination of "For Official Use Only" ("FOUO") material[181] stating:

> FOUO information may be disseminated within the DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function.[182]

An employee handling FOUO under this directive will be inclined to share FOUO with other Components of the DoD but will not do so upon the request of a non-DoD agency without first confirming that the other agency or government branch requesting the information is doing so for a "valid Government function." This term was not defined by DoD Regulation 5200.1. Utilizing Hypothetical One, the same DoD employee will share the requested CUI with the other agency if it is a part of DoD, but initially will not until the other agency's request is deemed to be a "valid function."

E. The "Mosaic Theory"

The idea that small bits and fragments of seemingly unimportant information can be combined to form an accurate "big picture" is known as the "Mosaic Theory."[183] If an enemy of the United States possessed the CUI discussed in Hypothetical One, he would know that, to ensure maximum carnage and structural damage, he should focus his attack on the Pentagon to target a wedge that does not contain the blast-proof windows described in the CUI. Perhaps an enemy would be less likely to launch an attack if some essential information were not available to use in formulating the attack plan, either as single piece of CUI, or as an aggregate of many pieces of CUI strung together.

---

[179] *Id.* at 14.

[180] Emmett Paige, Jr., Department of Defense Directive 5200.1–R (Jan. 14, 1997), http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf.

[181] This is an example of CUI indentified by the CUI TASK FORCE REPORT, *supra* note 20, at 33–34.

[182] Paige, Jr., *supra* note 180, app. 3 at 142.

[183] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 Yale L.J. 628, 630 (2005).

The Mosaic Theory is defined as:

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts.[184]

The intense focus on national security since the 9/11 Terrorist Attacks creates a perfect setting for agencies to employ the Mosaic Theory as a means of withholding pieces of information from disclosure.[185] The Mosaic Theory presents a fundamental challenge to transparency and the free flow of information sought by EO 13556; its greatest effect is on FOIA, a primary means for disclosure of government information.[186]

The concerns raised by the Mosaic Theory can be applied to CUI across the Executive Branch. Under the Mosaic Theory, the "appropriate unit of risk assessment" is the mosaic which could be formed should the piece of information in question be obtained by an adversary.[187] Government agencies have called upon Mosaic Theory concerns to classify documents at higher levels of sensitivity and to avoid disclosing documents for a variety of reasons.[188] These concerns have created a nearly unbeatable defense to disclosing documents and will prove to be a substantial challenge to the free flow of information called for by the Obama Administration.[189]

Nevertheless, a member of the public seeking CUI may choose to utilize a FOIA request to gain access to the information sought. When citizens and organizations seeking information take the appropriate steps to petition the government for release of desired information, EO 13556 stipulates that the "mere fact that information is designated as CUI shall not have a bearing on [disclosure] determinations . . . ."[190] This fact is crucial when considering how federal courts have ruled on FOIA claims in the past when agencies exert a defense based upon the Mosaic Theory. FOIA directs the United States District Courts to grant "substantial weight" when considering an agency's affidavit of

---

[184] *Id.*
[185] *Id.*
[186] *Id.* at 632.
[187] *Id.* at 633.
[188] *See id.* at 630 (stating that government agencies have used Mosaic Theory concerns to avoid FOIA and avoid pretrial discovery requests).
[189] *See id.* at 678–79; Goodwin, *supra* note 17, at 206–07.
[190] EO 13,556, *supra* note 19, § 2(b).

items to be kept secret under proper authority.[191] FOIA then affords agencies the same power to withhold disclosure of items recognized as CUI under EO 13556 through its enumerated exceptions.[192] Despite this directive, courts attempt to decide cases independently and without affording so much deference as to impede the exercise of justice.[193]

Federal courts, however, have been reluctant to probe agency explanations for the withholding of information on national security grounds.[194] When granting "substantial weight" to protected information, courts reason that agency expertise and their own lack of experience in dealing with national security matters affords the agency the right to prevent the disclosure of the information in question.[195] Although many of these claims are related to Exemption One of FOIA,[196] agencies can assert a claim for nondisclosure based on the Mosaic Theory that the release of CUI could help to build a picture that could be used to develop a threat to national security.[197]

Similar to the challenge of agency bias against information sharing, challenges to implementation under the Mosaic Theory have existed throughout the history of SBU.[198] In response to a March 19, 2002, White House Memorandum, NARA's ISOO and the Department of Justice's Office of Information and Privacy issued a memorandum ("NARA Memorandum")[199] urging agencies to consider FOIA Exemptions Two[200] and Four[201] when determining whether to categorize information as SBU.[202] Within the same

---

[191] Freedom of Information Act (FOIA), §5 U.S.C. 522(a)(4)(B) (2006).
[192] *Id.* at (b)(2)–(9).
[193] *See* Pozen, *supra* note 183, at 637 (listing cases and phrases from those decisions intended to show courts' independence but finding that the standard courts apply only test agency claims for "reasonableness, good faith, specificity, and plausibility").
[194] Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 Admin. L. Rev. 131, 163 (2006).
[195] *Id. See* Pozen, *supra* note 183, at 639; O'Reilly, note 6, at 822.
[196] Freedom of Information Act (FOIA) § 552(b)(1) (2006). Exemption One reads: "(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order[.]" *Id.*
[197] *See, e.g.* Pozen, *supra* note 183, at 630.
[198] *See generally* Knezo, *supra* note 56, at 23–25 (alluding to Mosaic Theory concerns of CUI/SBU disclosure).
[199] THE WHITE HOUSE, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, ACTION TO SAFEGUARD INFORMATION REGARDING WEAPONS OF MASS DESTRUCTION AND OTHER SENSITIVE DOCUMENTS RELATED TO HOMELAND SECURITY (Mar. 19, 2002), *available at* http://www.justice.gov/archive/oip/foiapost/2002foiapost10.htm.
[200] Freedom of Information Act (FOIA) § 552(b)(2) (2006).
[201] *Id.* § 552(b)(4).
[202] THE WHITE HOUSE, *supra* note 199, § III.

memorandum, the two offices cautioned that protecting sensitive information "from inappropriate disclosure should be carefully considered, on a case-by-case basis, *together with the benefits that result from the open and efficient exchange of scientific, technical, and like information*."[203] Along the same lines, in October 2001, Attorney General John Ashcroft issued a memorandum ("Ashcroft Memorandum")[204] instructing agencies to consider the interests the Bush Administration was committed to protecting when making discretionary disclosure decisions under FOIA.[205] In addition to changing the standard to which the Department of Justice would defend agency nondisclosure decisions under FOIA,[206] the Ashcroft Memorandum stated, "Such protection efforts [for critical infrastructure information], of course, must at the same time *include the protection of any agency information that could enable someone to succeed in causing the feared harm*."[207]

The language employed in both the NARA and Ashcroft Memoranda alludes to Mosaic Theory concerns; both memoranda call on agencies to consider outside information associated with a piece of CUI that is under request for disclosure.[208] Given the tendency of agencies to overprotect and the Bush Administration's reputation for secrecy in national security policy, agencies likely chose to withhold CUI from disclosure unless absolutely necessary. Like agencies' institutional bias against information sharing, these historical hurdles must be overcome to ensure effective implementation of CUI.

VI. RECOMMENDATIONS

As discussed, agencies have several concerns when it comes to sharing information with other agencies and the public, and these concerns will give pause to a security professional attempting to apply the most appropriate categorization to a piece of CUI. The vast amount of CUI documents across the Executive Branch will not all fit neatly into the various categories prescribed by NARA; some CUI will occupy a grey area that perplexes those who categorize a document and can potentially stifle its shareability between agencies and/or release to the public. Whether this inability to accurately assign a category comes from the contents of the CUI itself or from a lack of training or manpower,

---

[203] *Id.* (emphasis supplied).

[204] Memorandum from the Office of the Attorney Gen. on The Freedom of Information Act, (Oct. 12, 2001) *available at* http://www.doi.gov/foia/foia.pdf.

[205] *Id.*

[206] *See* Knezo, *supra* note 56, at 24 (describing that the Ashcroft memorandum replaced the predecessor FOIA memorandum of Janet Reno and replaced the "foreseeable harm" standard for information disclosure decision to that of a "sound legal basis" for nondisclosure).

[207] *Id.* at 25 (emphasis supplied).

[208] THE WHITE HOUSE, *supra* note 199, § III; Knezo, *supra* note 56, at 25.

it is crucial to find an appropriate category so the CUI can be properly safeguarded and disseminated.

A. Interagency Review Committee

During the past fifty years, various committees and commissions[209] have attempted to expose and rectify the problem of excessive overclassification—and therefore, the lack of public access—in the government but were largely ignored or produced only nominal effect.[210] However, a few of these bodies were successful and produced clear results.[211] The same need for transparency in and shareability of classified material across the government applies to CUI as well. In this section, recommendations to further ensure the most successful implementation of EO 13556 are elaborated.

The duration of classification and overclassification of information have long been issues of concern within the federal government.[212] In response to agency decisions not to declassify a document, the Interagency Security Classification Appeals Panel (ISCAP) was established to consider appeals from the public whose requests for declassification review were denied.[213] In 2009 alone, ISCAP declassified in full or in part sixty-nine percent of the documents appealed requesting declassication.[214] This figure remains consistent with the years preceding 2009, as ISCAP has declassified in whole or in part sixty-five percent of the documents, which were appealed for a declassification decision.[215] The surprise success of ISCAP, composed of Executive Branch officials, including those with the greatest interests in information security—the Department of

---

[209] Aftergood, *supra* note 1, at 404–06 (listing the 1956 Coolidge Committee, 1970 Defense Science Board Task Force on Secrecy, 1985 Stilwell Commission, 1994 Joint Secrecy Commission, 1997 Moynihan Commission, the 9/11 Commission, John F. Kennedy Assassination Records Collection Act, and the Nazi War Crimes Disclosure Act).

[210] *See id.* (discussing the numerous bodies which made suggestions but whose efforts were ultimately futile in reforming excessive secrecy on any level).

[211] *See id.* at 407–11 (explaining the successes of the Interagency Security Classification Appeals Council and the Department of Energy's Fundamental Classification Policy Review).

[212] *See id.* at 400–01 (stating that concerns about excessive secrecy in government have existed in the national security classification system for decades and that no significant reform has taken place in the past fifty years).

[213] Aftergood *supra* note 1, at 407; *see Interagency Security Classification Appeals Panel,* NAT'L ARCHIVES & RECORDS ADMIN., http://www.archives.gov/isoo/oversight-groups/iscap/ (last visited May 8, 2011).

[214] Info. Security Oversight Office, *2009 Report to the President* 21, (2010), http://www.archives.gov/isoo/reports/2009-annual-report.pdf.

[215] *Id.*

Defense, the Central Intelligence Agency, and the National Security Council[216]—proved to the federal government that a multiagency appellate body could effectively curtail the tendency of agencies to overprotect their information.

ISCAP demonstrates that, unlike the federal courts,[217] an individual seeking access to information has the odds in favor of gaining access to some or all of the information sought.[218] To properly address any CUI issues that may arise, the EA should establish a council like ISCAP—a "CUI Review Committee"—to hear a contested CUI categorization, either between the public and an agency or within an agency when it cannot assign an appropriate CUI category to a piece of CUI because of fears of the Mosaic Theory, unauthorized interception, loss of agency prestige, etc. Such a committee would effectively resolve any categorization or disclosure request problems in a neutral manner, allowing the appropriate balance to be struck between CUI protection and public access. The greatest advantage of an ISCAP model is that many executive agencies are represented, including those most concerned with protecting CUI and classified information, and can consider the request free of undue bias of the originating agency.

The decision reached by the CUI Review Committee, therefore, would reflect the decision of the Executive Branch agencies as a whole without fear of a particular agency's culture driving the result of the categorization. The CUI Review Committee could also serve as a forum for Executive Branch agencies to voice concerns and articulate suggestions to NARA. An alternative to forming a new CUI Review Committee, based on the success of ISCAP's declassification efforts throughout its existence, is the establishment of a second branch of ISCAP whose mission would be to resolve CUI-related issues. Either solution will likely grant the public access an improved process for access to information that Obama Administration and EO 13556 aim to provide.

B. Mandatory "Decategorization" Reviews

ISCAP spends much of its time reviewing Mandatory Declassification Reviews ("MDR").[219] MDR has proven to be a successful program; from 1996

---

[216] *Id.*

[217] *See, e.g.,* Pozen*, supra* note 183, at 636–38 (discussing how the courts defer classification decisions to the Executive Branch which practically ensures the government will prevail in FOIA litigation concerning national security).

[218] Info. Security Oversight Office, *2009 Report to the President* 21, (2010), http://www.archives.gov/isoo/reports/2009-annual-report.pdf.

[219] Info. Security Oversight Office, *2009 Report to the President* 11, (2010), http://www.archives.gov/isoo/reports/2009-annual-report.pdf ("Mandatory declassification review provides for direct, specific review for declassification of information when requested.").

through 2009, ninety-one percent of all requests were either wholly or partially declassified.[220] Such a rate of declassification increases public accessibility to previously unavailable material, and agencies, aware that the material has undergone MDR, share information without apprehension that the disseminated material will impact their missions. The proposed CUI Review Committee (or an expanded ISCAP) should process "decategorization" reviews to provide an inquiring public with the information it requests.

The mission of the CUI Review Committee should be to always strive for "smart" decategorization. To support the Obama Administration's call for openness, the CUI Review Committee will aim to make as much CUI accessible as possible, but it must use its collective expertise to regulate which material appropriate for dissemination even in the face of a president's call for unprecedented transparency.[221] Finally, if the CUI Review Committee finds that sharing and public access to information is stymied by the lack of an appropriate category, it must also have the power to solicit NARA to create the needed category. That is, if the CUI Review Committee finds that the CUI in Hypothetical One does not fit into any of the new categories created by NARA, it would then propose a new category with specifications for safeguarding and dissemination controls to be considered by NARA. Thus, the CUI Review Committee serves as a second safety net to ensure CUI is neither overprotected nor undercategorized.

C. Standardized Sanctions and Incentives

To ensure the uniform adherence of the EO 13556 directives across the government, each agency its employees must have an equal interest in the proper protection, marking, and goals of the new CUI schema. Agencies may achieve this status by adopting the recommendation of the CUI Task Force in regarding incentives and sanctions for employees.[222] In addition, once NARA's deadlines for implementation of the new CUI categorizations are determined, NARA must have some form of redress against agencies that repeatedly overprotect information where there is no compelling need.

---

[220] *Id.* at 15. MDR has proven to be a viable alternative to FOIA litigation. In fact, agencies have kept a backlog of requests since 1996. *Id.*

[221] Transparency and Open Government, 74 Fed. Reg. 4,685 (Jan. 26, 2009).

[222] *See* CUI TASK FORCE REPORT, *supra* note 20, at 23 (recommending that employ performance should be considered under the CUI Framework in evaluation, promotion, and award decisions and that agencies should be authorized to impose administrative sanctions for noncompliance with CUI policies or safeguarding requirements).

D. Training Uniformity

NARA will play a critical role in establishing training programs for information managers and the employees they oversee. Managers trained in EO 13556 compliance must successfully apply NARA's training within their own agency's culture without compromising its mission. The CUI Task Force recognizes that different levels of instruction are required based upon agency missions and employee duties and seniority.[223] Furthermore, the CUI Task Force recommends uniform "baseline" training, with agency training at the intermediate and advanced level to be coordinated between the individual agencies and the EA.[224] Finally, the CUI Task Force Reports suggests that agencies should be allowed to tailor their own training programs to meet the particular needs of their missions.[225]

NARA should take a more active role in developing training programs that can be uniformly applied to agencies across the Executive Branch; indeed, it must go beyond the CUI Task Force's recommendation and structure training programs that help ensure the maximum amount of CUI access is achieved. To accomplish this, NARA must have some influence over the training of intermediate and top-level government personnel in regard to the information sharing goals of EO 13556. More effective implementation also can be achieved by consulting agencies to identify their concerns about CUI and, consequently, developing a program that will instruct all employees at every level of seniority to effectively mark and share information. At every level of seniority, NARA's training should emphasize that the greatest level of CUI control should be employed only when absolutely necessary.

NARA should pay special attention of how CUI is marked and disseminated at different levels within agencies and then offer standardized instruction across all agencies to groupings of employees with similar levels of seniority. This allows individuals working in the same environment to be trained identically, allowing employees to exercise an "educated" individual judgment through benefit of standardized training. By implementing a uniform training program at every level of seniority, all agencies will receive identical instruction and seek to meet the goals of EO 13556 with minimum influence exerted by agency culture or bias.[226]

---

[223] *Id.* at 22.
[224] *Id.*
[225] *Id.*
[226] *See id.* at 29 (commenting that a lack of "standardized training," among other things, results in agencies tending to overprotect information).

Finally, each agency handling CUI should have an individual who oversees and ensures NARA training standards are not impeded by agency culture. To ensure the most effective implementation under EO 13556, NARA must have training oversight authority over these federal employees. Initially, NARA may draw these individuals from the agencies themselves. However, in order to prevent any unnecessary agency bias from affecting EO 13556's implementation, information managers must eventually be trained from the "ground up" by NARA and then be assigned as detailees to the agencies handling CUI.

E. National Archives and Records Administration

The sheer volume of information that qualifies as CUI across the federal government is enormous. To address the challenges it faces as EO 13556's EA, NARA must expand its staff to a level adequate to efficiently handle the workload. At this time, it is difficult to determine how many additional personnel will be required as NARA's duties as EA continue to develop and new directives are issued to facilitate implementation and compliance. The CUI Task Force concluded that, should the scope of CUI be expanded as it suggested, NARA would "need to provide extraordinary support to non-ISE agencies to ensure effective implementation of the CUI Framework."[227] EO 13556 expanded the scope of what constitutes CUI,[228] and, accordingly, NARA must be appropriately funded to carry out its mission, offer competitive salaries to attract the best public-sector information managers to its staff, and provide for the vehicles of implementation EO 13556 requires.

F. Notification to Non-federal Partners

An important part of fostering a continued understanding of CUI between the government and its partners, is keeping all the affected parties informed of new developments in CUI procedures. After the new CUI categories are established, each individual agency should adopt a "remarking" policy and associated deadline and should inform its government partners of the effective date of the changes. Timely notice will allow partners to immediately begin retraining their employees and formatting their marking programs to reflect changes in the marking categories of any CUI produced or owned by the partner. Agencies should therefore determine and announce their own implementation dates once they are certain their staff and resources can effectively mark, protect, and communicate the changes to their non-federal partners.

To facilitate the transition to using the new set of markings, agencies need to begin using the new categories as soon as possible and must ascertain

[227] *Id.* at 26.
[228] EO 13,556, *supra* note 19, § 2(a).

that their partners are aware of the absolute implementation deadlines[229] imposed by NARA. Early adoption of the new categories allows employees more time when becoming accustomed to the new categorizations and protections. In addition, upon implementation of the new categorizations, the executive agencies will need to communicate with their partners immediately to prevent CUI from being underprotected or overprotected by use of the former markings.[230]

VII. CONCLUSION

The challenges to the successful implementation of EO 13556 are numerous and complex. Agencies must overcome their own individual organizational biases that are resistant to information sharing while adjusting to a new "need to share" sensitive information policy. Deeply rooted in organizational culture, these biases favor overprotection rather than disclosure. Simultaneously, agency employees at all levels must be trained to comply with and further the goals of EO 13556. Meanwhile, ideas such as the Mosaic Theory and the potential compromise of sources and methods must be addressed; conflicts arising under the new standardized CUI schema will require an environment in which they can be discussed and resolved by those most strongly impacted by any decision made with regard to CUI policy. NARA must expand its staff and funding base, as well as assume a more pivotal role in the compliance process, from developing training programs to potentially administering sanctions where noncompliance is costly and chronic. Finally, state, local, tribal, and private sector government partners will need to be integrated into the new CUI marking and safeguarding process.

Public access to government information is essential to the democratic principles of the American Government, and the ability of agencies to share CUI across the government plays a vital role in the national security of the United States. EO 13556 is, in theory, a step in the right direction to accomplish the Obama Administration's goal of more transparency in government while simultaneously setting up a CUI framework that will allow information to be shared more often and more easily across the government. However, EO 13556 faces decades-old challenges to its successful implementation, as well as fresh, new ones---challenges which must be overcome before success can begin to be fully realized.

---

[229] *Id.* § 5(b).

[230] *See* O'Reilly, *supra* note 6, at 818 (suggesting that the federal government may be slow in communicating the changes to be implemented, thereby causing withholding of material whose release, in years past, had been routinely allowed or, conversely, allowing release of material whose disclosure, in years past, had been prohibited).