



TRADE SECRET

ORIGINATOR CONTROLLED

FOR INTERNAL USE ONLY

LIMITED ACCESS

RESTRICTED ACCESS

EXCLUDED FROM AUTOMATIC DOWNGRADING AND DECLASSIFICATION

SENSITIVE

SENSITIVE BUT UNCLASSIFIED

LIMITED DISTRIBUTION

FOR OFFICIAL USE ONLY

Report and Recommendations  
of the Presidential Task Force on

# CONTROLLED UNCLASSIFIED INFORMATION



# The Task Force on Controlled Unclassified Information



Under the leadership of:

**Janet Napolitano**  
Secretary of Homeland Security



**Eric H. Holder, Jr.**  
Attorney General



**Matthew L. Kronisch**  
Co-Chair  
Department of  
Homeland Security



**Candace Kelly**  
Co-Chair  
Department of Justice



**Dr. Josh Weerasinghe**  
Program Manager for the  
Information Sharing Environment



**Patricia Mantoan**  
Department of Health and  
Human Services



**Janice C. Haith**  
Department of Defense



**Michael A. Fitzpatrick**  
Office of Management  
and Budget



**Marguerite R. Coffey**  
Department of State



**John W. Vardaman**  
Department of Justice



**Greg Gardner**  
Office of the Director of  
National Intelligence



**William J. Bosanko**  
National Archives and  
Records Administration



**John J. Young**  
Department of  
Homeland Security



**Roland J. Corvington**  
Federal Bureau of Investigation



**Edwin J. McCeney**  
Department of the Interior



**Keith McElfresh**  
Department of Agriculture

**Patricia K. Hammar**  
Executive Secretary



# Table of Contents

Letter from the CUI Task Force Leadership

Executive Summary

CUI Task Force Recommendations

Part 1. Overview

- 1.1 The CUI Task Force
  - 1. Membership
  - 2. Methodology

Part 2. The SBU Challenge

- 2.1 Assessment of Current SBU Procedures
- 2.2 The 2008 CUI Framework

Part 3. Recommendations

- 3.1 Expanding the Scope of the Current CUI Framework
- 3.2 Measures to Enhance the Current CUI Framework
  - 1. Designation and Identification
  - 2. Marking
  - 3. Safeguarding
  - 4. Dissemination
  - 5. Life Cycle
  - 6. Exceptions
  - 7. Training
  - 8. Incentives and Accountability
  - 9. Standardization, Oversight, and Dispute Resolution
  - 10. Implementation Timeline and Resources
- 3.3 Measures to Track Progress in Implementation of CUI

Part 4. Conclusion

Appendix 1 Entities Consulted by the CUI Task Force

Appendix 2 SBU Markings Currently in Use

Appendix 3 List of Acronyms





August 25, 2009

The President  
The White House  
Washington, DC 20500

Dear Mr. President:

As directed by your May 27, 2009 Memorandum, we established an Interagency Task Force to review current procedures for categorizing and sharing Sensitive but Unclassified (“SBU”) information. The Task Force conducted a 90-day review of the Controlled Unclassified Information (“CUI”) Framework for terrorism-related information within the information sharing environment established by Presidential Memorandum in 2008, and considered whether that Framework should be expanded to apply to all SBU information under the control of the Executive Branch. Enclosed are the Report and Recommendations resulting from this review.

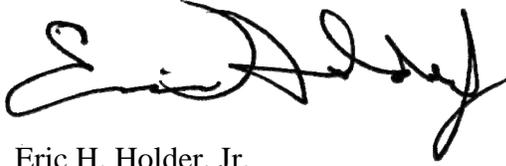
In addition to analyzing previous studies of SBU and the efforts of the CUI Council, the Task Force met with representatives from federal agencies both within and outside the information sharing environment; State, local, and tribal partners; privacy and open government organizations; and Congress. Informed by these consultations, a significant majority of the Task Force concluded that expanding the CUI Framework to encompass all SBU information will best strike the appropriate balance among the goals of Standardization, Information Sharing, and Government Transparency.

The recommendation of a vastly expanded scope for CUI necessitates a careful and coordinated effort to attain the benefits of standardization without adversely affecting agencies’ missions or the security of sensitive information. Accordingly, the report recommends a phased approach to implementation of the proposed CUI Framework that prioritizes training, marking, and oversight.

Taken as a whole, the Task Force’s recommendations seek to further information sharing among Executive Branch agencies as well as State, local, tribal and foreign partners by establishing a standard system for designating, marking, and handling all SBU information. The recommendations also enhance government transparency by establishing clear rules that protect information only when there is a compelling need to do so.

We recommend adoption of the Task Force Report and Recommendations, as well as the issuance of a new Executive Order rescinding the 2008 Memorandum on CUI and clearly setting forth the President's intention for this complex but important subject.

Respectfully,



Eric H. Holder, Jr.  
Attorney General



Janet Napolitano  
Secretary of Homeland Security

## Executive Summary

The President's Memorandum of May 27, 2009 on *Classified Information and Controlled Unclassified Information*, directed a Task Force, led by the Secretary of Homeland Security and the Attorney General, to review the Controlled Unclassified Information (“CUI”) Framework established in 2008 for the management of Sensitive but Unclassified<sup>1</sup> (“SBU”) terrorism-related information. The Task Force undertook a 90-day study of the CUI Framework, the current regimes for managing SBU information in the Executive Branch, and, by extension, the sharing of that information with our non-federal information-sharing partners.

The Task Force concluded that Executive Branch performance suffers immensely from interagency inconsistency in SBU policies, frequent uncertainty in interagency settings as to exactly what policies apply to given SBU information, and the inconsistent application of similar policies across agencies. Additionally, the absence of effective training, oversight, and accountability at many agencies results in a tendency to over-protect information, greatly diminishing government transparency.

Although the CUI Framework is intended to improve the sharing of only terrorism-related information, the Task Force concluded that a single, standardized framework for marking, safeguarding, and disseminating all Executive Branch SBU is required to further the goals of:

- standardizing currently disparate terminology and procedures (represented by over 107 distinct SBU regimes);
- facilitating information-sharing through the promulgation of common and understandable rules for information protection and dissemination; and
- enhancing government transparency through policies and training that clarify the standards for protecting information within the Framework.

A simple, concise, and standardized CUI Framework, with effective centralized governance and oversight has the best chance of both wide acceptance within the federal government and broad adoption throughout our State, local, tribal, and private sector partner communities. The successful expansion of the scope of the CUI Framework requires careful consideration of agency missions, requirements, and the processes by which SBU information is currently managed.

---

<sup>1</sup> Sensitive but Unclassified (SBU) information refers collectively to the various designations used within the Executive Branch for documents and information that are sufficiently sensitive to warrant some level of protection but that do not meet the standards for classification. CUI Framework refers to the single set of policies and procedures established by the Presidential Memorandum of May 7, 2008, governing the designation, marking, safeguarding, and dissemination of terrorism-related SBU information, which pursuant to that Memorandum, is renamed as “Controlled Unclassified Information.” Expanding the scope of the CUI Framework refers to the extension of the CUI Framework governing the designation, marking, safeguarding, and dissemination of CUI to all SBU information in possession or control of the Executive Branch.

Building upon the CUI Framework established in 2008, the Task Force has proposed 40 Recommendations intended to enhance Standardization, Information Sharing, Government Transparency, and the Protection of Information only where there is a compelling requirement to do so, including simplifying the definition of CUI; expanding the scope of the CUI Framework; clarifying that CUI markings have no bearing on releases either under the Freedom of Information Act or to Congress; and phasing implementation of the expanded scope of CUI.

## CUI Task Force Recommendations

Recommendation #1	Simplify the Definition of CUI
Recommendation #2	Expand the Scope of the CUI Framework
Recommendation #3	Make the Expanded CUI Framework the Exclusive Means of Protecting SBU
Recommendation #4	Adjust the CUI Council Membership and Roles to Reflect the Expanded Scope
Recommendation #5	Moratorium on New SBU Regimes
Recommendation #6	Engagement of Non-ISE Agencies
Recommendation #7	Phase Implementation of Scope Expansion
Recommendation #8	Designation of CUI
Recommendation #9	Identification of CUI
Recommendation #10	Agency CUI Programs
Recommendation #11	Simplification of Categories and Markings
Recommendation #12	Executive Agent to Establish Standard Markings and Guidance
Recommendation #13	Flexible Marking of CUI
Recommendation #14	Clarify that CUI Has No Bearing on FOIA
Recommendation #15	Safeguarding
Recommendation #16	Consultation on Threat
Recommendation #17	CIO Council as Advisor on Information Standards and Safeguards
Recommendation #18	Standardize Specified Dissemination
Recommendation #19	Dissemination to Congress and the Courts
Recommendation #20	Clarify Decontrol
Recommendation #21	Establish Life Cycle
Recommendation #22	Establish Exception Process
Recommendation #23	Delay in Incorporation of Exceptions into the CUI Framework
Recommendation #24	Amending Regulations or Statutes
Recommendation #25	Establish Training
Recommendation #26	Incentives
Recommendation #27	Accountability and Sanctions
Recommendation #28	Internal Oversight
Recommendation #29	Challenges to Designation and Identification
Recommendation #30	Federal Acquisition Guidance
Recommendation #31	Phase Implementation of Training, Marking, Oversight and Reporting
Recommendation #32	Phase Implementation of Technical Safeguards
Recommendation #33	Marking Initiation
Recommendation #34	Ensure Adequate Resourcing of Executive Agent
Recommendation #35	Synchronize CUI Implementation with Government Processes and Cycles
Recommendation #36	Impact of CUI on the Federal Enterprise Architecture
Recommendation #37	Incorporate CUI into Federal Grant Guidance
Recommendation #38	Annual Report of the Executive Agent
Recommendation #39	Establish a Baseline Measurement of Current SBU Efforts
Recommendation #40	Measure Implementation



## Part 1. Overview

In furtherance of the Administration's commitment to openness and transparency in government, the President's Memorandum of May 27, 2009, entitled *Classified Information and Controlled Unclassified Information* (the "2009 Memorandum") directed that the Attorney General and the Secretary of Homeland Security lead an Interagency Task Force on Controlled Unclassified Information ("CUI") (the "Task Force"). The mission of the Task Force was to review current procedures for categorizing and sharing Sensitive But Unclassified ("SBU")<sup>2</sup> information in order to determine whether such procedures strike the proper balance among certain imperatives. These imperatives include protecting legitimate security, law enforcement, and privacy interests as well as civil liberties; providing clear rules to those who handle SBU information; and ensuring that the handling and dissemination of information is not restricted unless there is a compelling need.

In addition to reviewing current procedures for SBU, the Task Force was charged with considering:

- measures to track agencies' progress with implementing the "CUI Framework"<sup>3</sup>
- other measures to enhance implementation of an effective information sharing environment across agencies and levels of government,<sup>4</sup> and
- whether the scope of the CUI Framework should remain limited to terrorism-related information within the Information Sharing Environment ("ISE") or be expanded to apply to all SBU information.

---

<sup>2</sup> As reflected in the 2009 Memorandum, SBU refers collectively to the various designations used within the Federal Government for documents and information that are sufficiently sensitive to warrant some level of protection, but that do not meet the standards for National Security Classification. A process created in 2005 for establishing a single, standardized, comprehensive categorical designation within the Executive Branch for most SBU information culminated with the adoption of the phrase "Controlled Unclassified Information" (CUI) in the Presidential Memorandum of May 7, 2008, entitled *Designation and Sharing of Controlled Unclassified Information* (CUI) (the "2008 Memorandum"). CUI was defined in the 2008 Memorandum 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.

The 2008 Memorandum directs that CUI be used in place of SBU as the single categorical designation for information within the scope of the CUI definition to refer generally to such information.

<sup>3</sup> The "CUI Framework" refers to the single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of terrorism-related CUI, as established in the 2008 Memorandum.

<sup>4</sup> Pursuant to the Memorandum of July 2, 2009, *Strengthening Information Sharing and Access*, the Assistant to the President for Homeland Security and Counterterrorism initiated a comprehensive review of the Information Sharing Environment. The Task Force was advised that it need not report on these measures.

## 1.1 The CUI Task Force

### 1. Membership

Led by the Secretary of Homeland Security and the Attorney General, and co-chaired by their senior representatives, the CUI Task Force was comprised of senior representatives of twelve federal agencies. This included representatives of following nine ISE agencies:

- Department of State (“State”)
- Office of the Director of National Intelligence (“ODNI”)
- Office of Management and Budget (“OMB”)
- Federal Bureau of Investigation (“FBI”)
- Department of Defense (“DoD”)
- Department of Health and Human Services (“HHS”)
- Program Manager, Information Sharing Environment (“PM-ISE”)
- Department of Homeland Security (“DHS”), and
- Department of Justice (“DOJ”).

The Task Force also included the following three non-ISE agencies:

- Department of Agriculture (“USDA”)
- Department of the Interior (“DOI”), and
- National Archives and Records Administration (“NARA”).

### 2. Methodology

The Task Force assessed current procedures for categorizing and sharing SBU, both within and outside of the ISE, in light of the imperatives specified in the 2009 Memorandum. The Task Force also analyzed the most significant issues thus far encountered by the Executive Agent (“EA”) and the CUI Council in developing the CUI Framework while recognizing the Task Force goals of standardization, information sharing, and government transparency. The Task Force drew upon SBU efforts dating back to 2006, as well as the CUI Council’s analysis, findings, draft policy statements, and implementation guidance as the foundation for much of its effort.

The Task Force met with representatives of multiple government entities to assess the many issues raised by implementation of the CUI Framework as described in the 2008 Memorandum, including its impact on agencies outside of the ISE, on the current exceptions to the CUI Framework,<sup>5</sup> on the ability of certain specific and discrete

---

<sup>5</sup> Four regimes for the safeguarding of infrastructure protection information were granted “excepted” status under the May 2008 Memorandum, including Protected Critical Infrastructure Information, Sensitive Security Information, Chemical Vulnerability Information, and Safeguards Information. Excepted status requires that the CUI Framework be used to the maximum extent possible, including the most applicable safeguarding marking, and that any additional safeguarding requirements beyond that specified under the CUI Framework shall be appropriately registered in the CUI Registry. Regulatory markings are to follow CUI markings and a specified dissemination instruction is to articulate any additional regulatory requirements.

communities of interest to support CUI implementation, and on the interests and concerns of Congress. The Task Force also met with representatives of a number of non-government entities to assess various aspects of CUI implementation on entities outside of the federal government, including private sector owners and operators of critical infrastructure, industrial security contractors, open government and privacy advocacy organizations, and our State, local, and tribal information sharing partners. (For a complete list of entities consulted, see Appendix 1.) These consultations were extraordinarily valuable in understanding the concerns of CUI constituents and were critical in developing the Task Force's recommendations.



## Part 2. The SBU Challenge

All federal agencies<sup>6</sup> routinely generate, use, store, and share information that, while not appropriate for “classification” under Executive Order 12958,<sup>7</sup> as amended, or other authority,<sup>8</sup> nevertheless requires some level of protection from unauthorized access and release. Protection may be required due to privacy concerns, law enforcement sensitivities, the business proprietary nature of the information, or for other reasons. Currently, across the Executive Branch, this information is identified by over 100 unique markings and at least 130 different labeling or handling regimes, such as “Law Enforcement Sensitive,” “For Official Use Only,” “Sensitive Security Information,” and “Limited Official Use.” (A partial listing of SBU markings is attached at Appendix 2.) Although SBU regimes or markings are typically derived from an identifiable authority, be it a statute, regulation, or agency policy, collectively they reflect a disjointed, inconsistent, and unpredictable system for protecting, sharing, and disclosing sensitive information.

### 2.1 Assessment of Current SBU Procedures

The Task Force reviewed current policies and procedures for categorizing and sharing SBU information to assess these processes against the imperatives identified by the President. The Task Force found that performance under these categories varied greatly. The factors influencing performance included the scope of subject matter and personnel covered; the intended purpose for control; the type of information protected; the process for developing policy and procedure; the clarity of policy and procedure; the availability of policy and procedure to persons handling subject information; the quality and frequency of employee training; and the existence of meaningful oversight. For some of these regimes, such as the widely utilized “Law Enforcement Sensitive” or “LES,” few of these factors are currently implemented.

Regardless of any individual regime’s performance, it is clear that as a whole, Executive Branch performance under these measures suffers immensely from interagency inconsistency in SBU policies, frequent uncertainty in interagency settings as to exactly what policies apply, and inconsistent application of similar policies across agencies.

---

<sup>6</sup> As used here and throughout the remainder of this report and its recommendations, the terms “agency,” “Agency,” or “agencies,” shall be deemed to refer to all Executive Branch departments, agencies, offices, components, and entities.

<sup>7</sup> See Exec. Order No. 12,958, 60 Fed. Reg. 19,823 (Apr. 20, 1995), reprinted as amended by Exec. Order 13292, 68 Fed. Reg. 15,315 (Mar. 28, 2003) (prescribing a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism).

<sup>8</sup> See *e.g.*, Atomic Energy Act of 1954, §§ 4 & 142, 42 U.S.C. §§ 2014(y) & 2162 (2009) (automatically classifying as “Restricted Data” all data concerning (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy; and automatically classifying as “Formerly Restricted Data” all data the Nuclear Regulatory Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as defense information).

Additionally, the absence of effective training, oversight, and accountability at many agencies results in a tendency to over-protect information as SBU, thus greatly diminishing government transparency.

Clarity as to what policies apply, as well as access to those policies, is essential to ensuring that a recipient properly handles SBU. Across the Executive Branch, the same type of information may be governed by entirely different, and often unclear, requirements. As a result, even where two agencies use the same marking, such as For Official Use Only (“FOUO”), and separately provide similar information to a recipient, that recipient must distinguish between the FOUO policies of each providing agency.

The Task Force recognized that sharing terrorism-related and other intelligence and law enforcement information with local law enforcement is critical to our national and homeland security.<sup>9</sup> Current SBU policies are generally ill-suited to this purpose. One example is when a State, local, or tribal official properly receives information from the federal government marked as “sensitive,” but does not receive any indication of the applicable safeguarding or dissemination policies. This situation can often result in the official’s reluctance to further share the information with other local law enforcement or first responders who may also have a need for it.

Another challenge presented by inconsistent, agency-specific SBU regimes is the incidental, yet often unintended effect some markings have on the processing of requests for public release of information under the Freedom of Information Act (“FOIA”). While a number of SBU regimes are based upon, or at least recognize, a specific statute or other legal authority for properly withholding information from public release under FOIA, many do not. Regardless, the markings are sometimes misunderstood as providing an independent basis for withholding documents from the public, Congress, or the courts, which in turn can undermine transparency, as well as public trust in government.

The lack of standardized Executive Branch procedures for governing SBU information is well-established,<sup>10</sup> the need for those standards well-documented,<sup>11</sup> and the interest of Congress to address the challenge, proven.<sup>12</sup>

---

<sup>9</sup> Final Report of the National Commission on Terrorist Attacks Upon the United States, www.9-11commission.gov.

<sup>10</sup> See e.g., The Constitution Project, *Reining in Excessive Secrecy: Recommendations for the Reform of the Classification and Controlled Unclassified Information Systems* (2009) available at <http://www.constitutionproject.org/manage/file/178.pdf>; U.S. Gov’t. Accountability Off., *Information Security: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements*, GAO-06-527T (Mar. 16, 2006); U.S. Gov’t. Accountability Off., *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Mar. 17, 2006); U.S. Gov’t. Accountability Off., *Managing Sensitive Information: DOE and DOD Could Improve Their Policies and Oversight*, GAO-06-531T (Mar. 14, 2006); U.S. Gov’t. Accountability Off., *TSA: Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO-05-677 (Jun. 29, 2005); U.S. Gen. Acct. Off., *Selected Agencies’ Handling of Personnel Information*, GAO-02-1058 (Sep. 30, 2002); Cong. Res. Serv., *‘Sensitive but Unclassified Information’ and Other Controls Policy and Options for Scientific and Technical Information*, CRS Rep. RL31845 (Feb. 15, 2006), as updated by CRS Rep. RL33303 (Dec. 29, 2006); Cong. Res. Serv., *Secrecy vs. Openness: New Proposed Arrangements for Balancing Competing Needs*, CRS Rep. 21895 (Aug. 26, 2004), as updated (Oct. 12, 2004).

## 2.2 The 2008 CUI Framework

Although the problems associated with SBU have existed for many decades, addressing them assumed greater urgency following the information sharing failures preceding the 9/11 attacks. The 9/11 Commission reported that in the months leading up to the attacks:

Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled . . . Often the handoffs of information were lost across the divide separating the foreign and domestic agencies of government.<sup>13</sup>

In response to these challenges, in 2004, Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act, Pub. L. 108-458, which mandated the development of an Information Sharing Environment (“ISE”) to facilitate the sharing of terrorism-related information among federal, State, local, tribal, private sector, and foreign partner entities. On December 16, 2005, President Bush directed federal agencies to recommend procedures for standardizing the marking, handling, and safeguarding of SBU information.<sup>14</sup> The resulting recommendations<sup>15</sup> were largely reflected in the 2008 Memorandum, which adopted CUI as the single Executive Branch designation for all SBU within the scope of the ISE, and established a corresponding new framework for designating, marking, safeguarding, and disseminating terrorism-related CUI, which became known as the CUI Framework.<sup>16</sup>

The 2008 Memorandum designated the National Archives and Records Administration (NARA) as the Executive Agent (EA) for the CUI Framework and directed that a CUI Council<sup>17</sup> perform an advisory and coordinating role for the development of policy

---

<sup>11</sup> Final Report of the National Commission on Terrorist Attacks Upon the United States, [www.9-11commission.gov](http://www.9-11commission.gov), 416-419.

<sup>12</sup> See e.g., the “Reducing Over-Classification Act of 2009,” H.R. 553, 111th Cong. (1st Sess. 2009) (as introduced by Rep. Harman, Jan. 15, 2009); the “Reducing Information Control Designations Act,” H.R. 1323, 111th Cong. (1st Sess. 2009) (as introduced by Rep. Driehaus, Mar. 5, 2009); the “Implementing the Controlled Unclassified Information Framework Act of 2008,” S. 3662, 110th Cong. (2nd Sess. 2008) (as introduced by Sen. Lieberman, Oct. 1, 2008); the “Reducing Overclassification Act of 2008,” H.R. 4806, 110th Cong. (2nd Sess. 2008) (as introduced by Rep. Harman, Dec. 18, 2007); the “Improving the Public Access to Documents Act of 2008,” H.R. 6193, 110th Cong. (2nd Sess. 2008) (as introduced by Rep. Harman, Jun. 5, 2008); and the “Reducing Information Control Designations Act,” H.R. 6576, 110th Cong. (2nd Sess. 2008) (as introduced by Rep. Waxman, Jul. 23, 2008).

<sup>13</sup> Final Report of the National Commission on Terrorist Attacks Upon the United States, [www.9-11commission.gov](http://www.9-11commission.gov), 353.

<sup>14</sup> Memorandum for Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment, December 16, 2005. This Memorandum requires the development of recommendations, first, for homeland security information, law enforcement information, and terrorism information and then for all types of information not previously addressed.

<sup>15</sup> Presidential Guideline 3 Report, Standardized Procedures for Sensitive But Unclassified (SBU) Information, (Fall 2007).

<sup>16</sup> 2008 Memorandum, at 4-6.

<sup>17</sup> The CUI Council was established by the National Archives and Records Administration (NARA) in accordance with the 2008 Memorandum, as a subcommittee of the Information Sharing Council (ISC) created by the Intelligence Reform and Terrorism prevention Act of 2004 (Public Law 108-458) (IRTPA). Guidance issued separately by the PM-ISE on July 9, 2008, directed each ISC agency to designate a

standards and implementation guidance for the CUI Framework. With a May 2013 deadline for full implementation of the CUI Framework, the Archivist of the United States established the CUI Office, which hosted the first monthly meeting of the CUI Council in August 2008.

In the ensuing 12 months, the EA, in consultation with the CUI Council, has conducted data calls and analyses, initiated the development of an implementation plan along with draft guidance in key policy areas, including: designation, marking, dissemination, safeguarding, dispute resolution, life cycle, oversight, and exceptions. As a result of these efforts, the emerging CUI Framework is intended to include: a standing Governance Structure under the current EA; two possible levels of safeguarding;<sup>18</sup> two possible levels of dissemination controls;<sup>19</sup> a procedure for designating specific dissemination requirements or limitations, when appropriate; three unique markings to reflect the three combinations of safeguarding and dissemination controls;<sup>20</sup> a publicly available, web based “Registry” of markings that apply to CUI information and certain associated policies; and standardized training requirements across the federal government.

Although implementation of the CUI Framework will be required only within the Executive Branch, it is intentionally being developed to be as accessible as possible to non-federal information sharing partners, such as State, local, tribal, and foreign governments and the private sector. Thus, the promulgation and publication of standard rules across the Executive Branch should not only ease the handling of CUI by our non-federal partners, but it could also encourage the adoption of these rules and facilitate compliance with similar rules by partners outside the Executive Branch. Although adoption by non-federal partners may require modifications to accommodate applicable State, local and tribal law, in meeting with the Task Force, State, local and tribal representatives nonetheless expressed their desire to see the CUI Framework achieve the same broad acceptance and adaptation experienced by the Rules for Criminal Intelligence System Operating Policies promulgated by the Department of Justice.<sup>21</sup>

---

representative to the CUI Council. The CUI Council effectively represents the needs and equities of ISE participants, providing the EA with advice and recommendations on CUI policies. The membership of the CUI Council currently includes: Department of Commerce, Department of Defense (Office of the Secretary and Joint Staff), Office of the Director of National Intelligence (on behalf of the Intelligence Community), Department of Energy, Federal Bureau of Investigation, Department of Health and Human Services, Department of Homeland Security, Department of the Interior, Office of Management and Budget, Department of Justice, Program Manager for the Information Sharing Environment, Department of State, Department of Transportation, Department of The Treasury, Environmental Protection Agency, and the Nuclear Regulatory Commission. In addition, non-federal participation on the CUI Council includes two members from State, local, and/or tribal government, two members from the private sector, and consultation with the ISC’s State, Local, Tribal, and Private Sector Subcommittee, as appropriate.

<sup>18</sup> “Safeguarding” means measures and controls to protect CUI from unauthorized access resulting from theft, trespass, or carelessness. The current safeguarding levels are “Controlled” and “Controlled Enhanced.”

<sup>19</sup> Dissemination controls are instructions governing the extent to which dissemination is permitted or limited. The current dissemination controls are “Standard Dissemination” and “Specified Dissemination.”

<sup>20</sup> The markings include “CONTROLLED WITH STANDARD DISSEMINATION”, “CONTROLLED WITH SPECIFIED DISSEMINATION”, and “CONTROLLED ENHANCED WITH SPECIFIED DISSEMINATION.” At this time, there is no anticipated marking category that would couple “Controlled Enhanced” safeguards with “Standard Dissemination” controls.

<sup>21</sup> See “Criminal Intelligence Systems Operating Policies,” 28 C.F.R. pt. 23 (2009). 28 C.F.R. part 23 is a guideline for federal, State, and local law enforcement agencies to follow in implementing standards for

## Part 3. Recommendations

### 3.1 Expanding the Scope of the Current CUI Framework

The CUI Task Force was specifically directed to consider whether the scope of the CUI Framework should remain limited to terrorism-related information within the ISE, or, be expanded to apply to all SBU information, and by extension, apply beyond the realm of the ISE.

Eleven of the 12 Task Force members concurred in the recommendation to expand the scope of the CUI Framework beyond the ISE and to all SBU information.<sup>22</sup> Even prior to the establishment of the Task Force, DHS and DOD, as well as the FBI and ODNI (on behalf of the National Intelligence Community) had already committed to extending the current CUI Framework to all SBU within their control. It was the consensus of the 11 concurring agencies that maintaining multiple regimes for managing SBU information would be inconsistent with the goals of the Task Force, and that expanding the scope of the current CUI Framework would provide for specificity and consistency in the marking and identification of various types of sensitive information.

A number of Task Force members also endorsed expanding the scope of the current CUI Framework as a means of providing greater clarity in implementation. For example, although the 2008 Memorandum's definition of "CUI" is not limited to terrorism-related information, the scope of the CUI Framework it established is limited to terrorism-related information. Maintaining this discrepancy would force agencies to perform the often difficult task of segregating terrorism-related from non-terrorism-related information, a distinction that is not always clear or static.

The Task Force believes the first step in improving the CUI Framework is to simplify the definition of CUI. CUI should be defined as "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." Next, the scope of the CUI Framework should be expanded to include all information falling within the definition of CUI in the possession or under the control of the Executive Branch. As directed in the 2008 Memorandum, CUI should be used in

---

operating federally grant-funded multi-jurisdictional criminal intelligence systems. It was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. It provides specific guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process. Only information technology systems operating under or funded through the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3711, et seq., as amended, must comply with the 28 C.F.R. part 23; however, the underlying "framework" has been widely applied to other activities involving the collection, maintenance, and dissemination of criminal intelligence information.

<sup>22</sup> The Department of State opposes scope expansion out of concern that it would dilute the terrorism-related focus of the Framework envisioned in the 2008 Memorandum and the ability to use the CUI marking as a means of identifying solely terrorism-related information.

place of SBU as the single categorical designation for all information falling within the scope of the definition of CUI.

In sum, a strong majority of the Task Force believes that limiting the scope of the CUI Framework to terrorism-related information within the ISE: (1) risks overlooking information with a terrorism nexus that may not be apparent until some later time; (2) fails to address the inefficiencies and confusion in continuing to maintain over 100 discrete SBU markings across the federal government; (3) could result in unintended inefficiencies, such as where agencies that handle sensitive terrorism-related and non-terrorism-related information would have to maintain at least two separate systems for handling SBU; and (4) creates confusion as to the true scope of CUI.

Expanding the scope of the CUI Framework is not intended to provide agencies with unfettered access to all the sensitive unclassified information within the Executive Branch; rather, it is meant to facilitate appropriate sharing of sensitive unclassified information. It would also promote increased accountability in how information is shared by allowing agencies and the public to know what kind of information is maintained by federal agencies.

Moreover, because of its uniformity, standardized training requirements, and the public availability of the registry, the expanded scope of the CUI Framework can be expected to significantly increase the openness and transparency of government by improving the efficiency of information sharing, where otherwise authorized, between and among federal, State, local, tribal, private sector, and foreign partners. By eliminating the overuse of SBU designations, an expanded CUI Framework would enhance the protection of personal privacy and civil liberties, while continuing to protect sensitive information as appropriate.

The Task Force believes that the efforts of the EA and the CUI Council are enhanced when taking into consideration the perspectives of a wide range of information-sharing partners and incorporating those perspectives into policy development efforts. The EA could achieve this by periodically inviting public interest or private sector entities to attend meetings for the purpose of providing their insights, experiences, observations or opinions on relevant matters.

The Task Forces believes that expansion of the CUI Framework necessitates an expansion of the CUI Council membership, which, under the 2008 Memorandum, was limited to members of the Information Sharing Council,<sup>23</sup> as well as to its roles and functions. Composition of the CUI Council should be adjusted to reflect the scope of CUI under an expanded CUI Framework. To accommodate that expanded scope while optimizing effective representation, the Task Force believes the core composition of the Council should primarily include “capstone” agencies. For example, ODNI would represent all intelligence community agencies; DOD would represent each of the military services and all other DOD elements; DHS would represent all of the component agencies of DHS; DOJ would represent its subordinate agencies, etc. The expanded CUI Council should be recognized as a consensus body for developing CUI policy and should retain the

---

<sup>23</sup> The Information Sharing Council has been merged into the Information Sharing and Access Interagency Policy Committee.

responsibilities and authorities identified in the 2008 Memorandum, including resolving disputes among agencies concerning the proper designation or marking of CUI. In addition, the Task Force believes that the CUI Council should be empowered to hear appeals from agency dispute/challenge mechanisms.

The majority of developments in post 9/11 information sharing have impacted terrorism-related information within the context of the ISE. Agencies outside of the ISE have generally had only limited exposure to the CUI Framework directed by the 2008 Memorandum. Task Force outreach to those agencies identified the steeper learning curve many of them would face in implementing the CUI Framework as compared to their peers within the ISE. To begin to understand non-ISE agency requirements, the Task Force believes that the EA should reach out to these agencies and inform them of efforts to implement the Framework in light of the 2008 Memorandum and the recommendations contained herein. The EA should solicit from them any agency-specific needs or considerations relevant to their implementation of the CUI Framework.

### ***Recommendation #1 Simplify the Definition of CUI***

The definition of “Controlled Unclassified Information,” or CUI, should 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.

### ***Recommendation #2 Expand the Scope of the CUI Framework***

The scope of the CUI Framework should be expanded to include all information falling within the definition of CUI in the possession or under the control of the Executive Branch of the Federal Government.

### ***Recommendation #3 Make the Expanded CUI Framework the Exclusive Means of Protecting SBU***

The expanded CUI Framework should be the single categorical designation used to identify, safeguard, and disseminate unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls, except where a particular regime has been approved by the EA as a temporary exception to the CUI Framework.

### ***Recommendation #4 Adjust the CUI Council Membership and Roles to Reflect the Expanded Scope***

CUI Council membership should be adjusted to reflect the expanded scope of the CUI Framework, and membership reassessed to prioritize representation through “capstone” agencies. Additionally, the CUI Council should be empowered to address appeals of agency dispute/challenge mechanisms.

### **Recommendation #5 Moratorium on New SBU Regimes**

Consistent with the imperatives listed in the 2009 Memorandum, the President should impose a moratorium on efforts within the Executive Branch to define or develop new SBU categories outside of the CUI Framework.

### **Recommendation #6 Engagement of Non-ISE Agencies**

The EA should develop a 120-day outreach plan to engage all non-ISE agencies in CUI Framework efforts and the EA should solicit from them any agency-specific needs or considerations relevant to their implementation of the CUI Framework.

### **Recommendation #7 Phase Implementation of Scope Expansion**

Implementation of the CUI Framework should begin with all ISE agencies, and consistent with the 2008 Memorandum, they should complete implementation by May 2013. All other agencies (other than the excepted regimes) should complete implementation by May 2015. The excepted regimes should complete implementation by May 2016. If the excepted regimes believe that implementation by May 2016 would cause serious and demonstrable harm, they may petition the EA, upon identification of their specific concerns and proposals for their remediation, for an extension of time to ensure that exception implementation does not negatively impact those regimes.

## **3.2 Measures to Enhance the Current CUI Framework**

The discussions and recommendations which follow are intended to improve the current CUI Framework, as established in the 2008 Memorandum.

### **1. Designation and Identification**

Since issuance of the 2008 Memorandum, the EA, in coordination with the CUI Council, has worked to define the concepts of “Designation” and “Identification.” *Designation* is currently defined as the determination that a general category of information (e.g. personally identifiable information, law enforcement information, etc.) may be protected as CUI and, if so, the level of protection required and dissemination authorized. It is each agency’s responsibility to evaluate its data holdings to determine what information should be designated as CUI. It is foreseeable, based on the revised definition and scope of CUI recommended herein, that some information currently treated as “sensitive” may be found not to warrant CUI designation. Designation may be initiated by the President, statute, regulation, agency head, or appropriately designated senior agency official. *Identification* is currently defined as recognition by an authorized individual that specific information fits within a general category of information which has been previously *designated* as CUI.

A key goal of the expanded CUI Framework is reducing the number of existing SBU regimes into the minimum appropriate number of CUI designations. The EA, in

coordination with the CUI Council, has already begun the process for designating various general categories of information common to most agencies, including:

- Acquisition-Related Information
- Law Enforcement
- Export Controlled
- Business Proprietary
- Intellectual Property Controls
- Privacy Protected Information
- Restrictions on Non-U.S. Citizens
- Legal Privileges and Restrictions
- Security Information

#### *Accommodation and Flexibility*

In exercising their respective responsibilities, the EA and CUI Council should fully consider the mission and requirements of the agency recommending a designation and make all appropriate efforts to accommodate those requirements in the harmonization effort. Similarly, senior officials of agencies recommending designations should be flexible in working with the EA to ensure that harmonization of their designation recommendations with the CUI Framework is achieved.

#### **Recommendation #8 Designation of CUI**

CUI designation by the EA should reflect the following four-step process:

Step 1: The agency head, or other appropriately designated senior-level official, determines that there exists a compelling requirement to protect a category of information that the agency routinely handles, and which has not already been designated by the EA.

Step 2: The official submits a designation recommendation, along with supporting and accompanying materials (e.g., statute, regulation, or policy), to the EA for review and consideration.

Step 3: In consultation with the CUI Council, the EA reviews the designation recommendation for the purpose of ensuring that:

- a. the description of, authority and justification for, and requested standards for safeguarding and dissemination are clearly articulated;
- b. the requested designation is consistent with standards applicable to any similar types of information and harmonized, as appropriate, with those designations; and

- c. the submitting agency is aware of and understands any concern of the EA, or of any other agency, that a prospective designation does not warrant the protection levels selected and/or the ensuing loss of government transparency accompanying designation.

Step 4: Upon approval by the EA, designations and supporting information are published, as appropriate, to a public CUI Registry, from which the public and official users of CUI markings may identify the categories of information designated as CUI. To the extent that any of the information supporting a particular designation is, itself, CUI, it will be maintained separately from the public registry by the EA.

### ***Recommendation #9 Identification of CUI***

Each agency should establish standards for personnel possessing the authority and/or necessary qualifications for identifying information as CUI. At a minimum, all individuals authorized to identify CUI should meet standardized CUI training requirements, as implemented within that agency.

### ***Recommendation #10 Agency CUI Programs***

Each agency should establish a program to manage its CUI. The program should include, at a minimum, Senior Officials responsible on behalf of the agency head for recommending CUI Designations, providing training, CUI management, and oversight of agency CUI activities.

## **2. Marking**

### *Standardization of Markings*

Standardization is one of the goals of CUI implementation. The EA should provide the standardized markings and marking requirements with which agencies will comply. The decision regarding how to apply the standardized CUI markings to the various forms of CUI should be left to agency discretion. CUI intended for dissemination must be marked, but agency mission, intended data usage, access policies, established information exchange processes, and means or purposes for disseminating should all inform the agency decision regarding the most appropriate means of marking.

EA approved standardized markings should identify CUI designation, safeguarding and dissemination controls; originating agency; and life cycle, and should be the only markings used to convey this information. The Task Force reviewed the many variations of markings and marking schemes employed in the legacy SBU regimes and concluded that no marking scheme in current use can accommodate all requirements of the expanded scope. For example, some agencies – particularly those outside of the ISE – routinely process and transfer bulk form SBU (e.g., privacy, health, income, etc.) with other

agencies, but for a very limited purpose, to a known and limited audience, and under clear processes. In such circumstances, it is possible that simply using a “system-high”<sup>24</sup> marking may be adequate. Alternatively, in the case of finished intelligence products intended for dissemination to our State, local, and tribal partners, it may be irresponsible not to clearly identify the intelligence report as CUI, and to include any warranted portion marking. The Task Force recognized the value of some level of portion marking for specific formats of CUI in information sharing efforts to enable the ready identification of the CUI elements within appropriately marked documents.

The Task Force believes that agencies should consider the full range of marking options – including, as appropriate, system-high, database, application, document, portion, paragraph, and data element identification<sup>25</sup> - as required by mission and information protection and sharing requirements. When shared, all information should be marked consistent with EA issued standards.

Given the likelihood that mission requirements may necessitate occasional deviations from the standards, the EA should be authorized to waive or modify these standards in such circumstances.

### *Simplification of Markings*

The Task Force believes that the CUI Framework, not only across federal agencies, but in the potential for its adoption by State, local, tribal, private sector, and foreign partners, requires the use of terminology which is clear, simple and intuitive. It is likely that while the 2008 Memorandum’s categorizing scheme is appropriate, its supporting marking nomenclature (“CONTROLLED WITH STANDARD DISSEMINATION,” “CONTROLLED WITH SPECIFIED DISSEMINATION,” and “CONTROLLED ENHANCED WITH SPECIFIED DISSEMINATION”) can be improved. The Task Force encourages the EA to utilize input from a variety of CUI user focus groups, to try out variations of markings or labels and facilitate development of standard markings. The Task Force believes CUI markings should use plain language, and while abbreviations are appropriate, codes should be discouraged.

### *Public Registry*

The Task Force views the public registry as an important source of government transparency and public insight into CUI designations. While the CUI registry would contain a full description of the requirements for safeguarding and disseminating CUI, the Task Force nonetheless believes it preferable that a given CUI document (such as an intelligence report) itself, to the extent possible, contain any safeguarding and dissemination information necessary to its proper handling.

---

<sup>24</sup>System High is a means of marking an entire system at the level of the most restricted CUI within the system.

<sup>25</sup>Database marking would identify the most restricted CUI at the database level. Application marking would identify the most restricted CUI at the application level. Document marking would identify the most restricted CUI within a document. Paragraph or portion marking would identify each paragraph or portion containing CUI at the most restricted level found in that paragraph or portion. Data element identification includes the marking only of those discrete data elements or segments of information that are deemed CUI.

### *Distinguish from FOIA*

Finally, the Task Force believes it is critical to recognize that the CUI Framework does not alter the requirements of FOIA, and that CUI implementation guidance and training make clear that the presence or absence of a CUI marking has no bearing on whether a record is releasable or exempt from release under FOIA.

### ***Recommendation #11 Simplification of Categories and Markings***

The 2008 Memorandum marking nomenclature should be replaced with succinct, informative overall markings, such as:

- CONTROLLED-ENHANCED
- CONTROLLED-SPECIFIED
- CONTROLLED-STANDARD
- or
- CONTROLLED-HIGH
- CONTROLLED-MEDIUM
- CONTROLLED-LOW

### ***Recommendation #12 EA to Establish Standard Markings and Guidance***

The EA should establish standardized CUI markings that identify CUI designation, safeguarding and dissemination controls; originating agency; and life cycle. The EA should publish the standardized markings and marking guidance to the agencies. Upon agency request, the EA may grant specific waivers or modifications to these standards, and the EA should work with agencies to ensure compliance with both the Framework and agency requirements.

### ***Recommendation #13 Flexible Marking of CUI***

CUI intended for dissemination must be marked in accordance with the standardized markings established by the EA. Agency decisions regarding how and when to apply standardized CUI markings should consider the full range of marking options and be driven by agency mission, the medium in which the CUI resides or is conveyed, and information protection and sharing requirements.

### ***Recommendation #14 Clarify that CUI Has No Bearing on FOIA***

CUI implementation guidance and CUI training should make clear that the CUI Framework and FOIA are entirely separate and that CUI markings have no bearing on whether records are exempt from release under FOIA.

### 3. Safeguarding

“Safeguarding” refers to physical or electronic measures that ensure CUI is not accessed inadvertently or improperly. The two levels of safeguarding established in the 2008 Memorandum, “standard”<sup>26</sup> and “enhanced”,<sup>27</sup> are believed adequate for the expanded scope of the CUI Framework proposed herein. The Task Force is concerned, however, that incorporating existing federal IT standards directly into the CUI Framework could pose a significant impediment to CUI implementation, as application and adherence have been inconsistent to date. The reasons for the inconsistency include cost, complexity, and some contradiction between overlapping rules.

Mindful of the fact that agencies are obligated to comply with federal IT standards independent of those standards’ inclusion in the CUI Framework, the Task Force has concluded that the EA, in consultation with the Federal Chief Information Officer (CIO) Council, should develop IT safeguarding standards for the CUI Framework in a phased manner.

The Task Force endorses the position of OMB that phased development of IT standards for the CUI Framework is neither authority for nor endorsement of non-compliance by agencies with federal IT standards. The Task Force believes that Federal CIOs, through the Federal CIO Council, could provide relevant, practical, and objective advice and perspectives given their current responsibilities across government for balancing security requirements with IT planning and implementation. Assistance in aligning metadata tagging and digital identity management with the CUI Framework to manage access to CUI is one goal for such advice.

An additional safeguarding challenge arises when sensitive federal government information is shared with State, local, tribal, private sector, and foreign partners. As non-federal partners, these entities are neither required by law to comply with the same physical or IT safeguarding standards as the federal Executive Branch, nor are they necessarily funded to do so. Nonetheless, the Task Force believes that non-federal entities that receive CUI from the federal government should be encouraged to provide safeguarding protection consistent with the CUI Framework to the maximum extent possible.

Recognizing the need to achieve the parallel goals of information protection and information sharing with these partners, the Task Force concluded that the CUI Framework would likely benefit from the establishment of standardized arrangements to address formal, recurring, and institutionalized information sharing settings as well as informal, irregular, or field conditions. Such means must be based on risk management as informed by operational requirements.

---

<sup>26</sup> “‘Standard Safeguarding’ is a handling instruction that means the information so designated is subject to baseline safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure.” 2008 Memorandum, at 3.

<sup>27</sup> “‘Enhanced Safeguarding’ is a handling requirement that means the information so designated is subject to measures more stringent than those normally required because inadvertent or unauthorized disclosure would create a risk of substantial harm.” 2008 Memorandum, at 2.

There are useful precedents for formal information sharing arrangements between the federal government and non-federal partners. Despite certain obvious distinctions between them and the CUI Framework, the Task Force was impressed by the procedures implemented by the Chemical-Terrorism Vulnerability Information (“CVI”)<sup>28</sup> and Protected Critical Infrastructure Information (“PCII”)<sup>29</sup> programs. Both of those programs have well developed guidelines, tailored to mission needs, providing safeguarding standards which can be achieved with reasonable and appropriate efforts by the non-federal partners. The PCII program also contains an “Accreditation” process. The Task Force encourages the EA and CUI Council to review those procedures for any appropriate measures which may benefit the CUI Framework, taking proper account of situations in which non-federal partners may have severe resource constraints.

Information sharing which is informal, irregular, or which occurs under field conditions presents its own set of safeguarding concerns, and in these circumstances, formal procedures, agreements, and compliance mechanisms may serve only to impede information sharing. The Task Force believes that in such circumstances, where information must be shared, but where there is no opportunity for formalizing procedures, federal employees and their non-federal partners should be enabled to identify “equivalent measures,” taking into account the sensitivity of the particular CUI and the risks thereto. In such circumstances, a federal employee’s training and understanding of the CUI Framework could be critical, both to ensure protection of the information, and to ensure that sharing is not impeded by “non-issues.” The Task Force would encourage agencies to develop pocket reference cards and short-form CUI Agreements for use by personnel in the field.

### ***Recommendation #15 Safeguarding***

The EA, in consultation with the CUI Council, should develop a means to address safeguarding in formal, recurring, and institutionalized information sharing settings, as well as in informal or irregular situations including field conditions.

### ***Recommendation #16 Consultation on Threat***

The EA, in consultation with the CUI Council, should consult with appropriate entities to determine the level at which certain unclassified information on federal government networks and systems is being targeted in order to best allocate resources to protect CUI.

---

<sup>28</sup> Procedures for the CVI program can be found in the CVI Manual, [http://www.dhs.gov/xlibrary/assets/chemsec\\_cvi\\_proceduresmanual.pdf](http://www.dhs.gov/xlibrary/assets/chemsec_cvi_proceduresmanual.pdf)

<sup>29</sup> Procedures for the PCII program can be found in the April 2009 Protected Critical Infrastructure Information Program Procedures Manual, found at [http://www.dhs.gov/xlibrary/assets/pcii\\_program\\_procedures\\_manual.pdf](http://www.dhs.gov/xlibrary/assets/pcii_program_procedures_manual.pdf)

## **Recommendation # 17 CIO Council as Advisor on Information Standards and Safeguards**

The EA should utilize the Federal CIO Council for advice and consultation on:

- a. appropriate measures to support a phased approach to the application of information technology standards to the CUI Framework,
- b. a balanced set of technology requirements for safeguarding CUI which are consistent with federal guidance and achievable by our non-federal information sharing partners, and
- c. metadata standards to promote transparency, facilitate IT functions, and support digital privilege management.

### **4. Dissemination**

The CUI Framework currently contains two dissemination controls - “Standard” and “Specified.” Standard dissemination control allows an authorized holder, based on his/her discretion, to provide the CUI to federal, State, local, tribal, private sector, and foreign partners – provided that the dissemination furthers an official mission purpose. Specified Dissemination rules are used when there are compelling requirements to limit the authorized holder’s discretion. Specified dissemination requires additional markings describing those limits. These restrictions, based on law, regulation, interagency or intergovernmental agreement, or agency policy, should define a specified dissemination instruction clearly articulating the discretion authorized the holder, as approved by the EA at designation. Where CUI is marked only to identify it as CUI, without specifying dissemination instructions, standard dissemination applies. Where specified dissemination rules do not lend themselves to effective summarization, they will be maintained by the EA and made easily accessible to handlers of that category of CUI.

#### *Congress and the Judiciary*

While the CUI Framework may well include a designation for materials covered by Executive Privilege, the Task Force recognized that Executive accountability requires that CUI markings do not themselves interfere with the checks and balances provided by the legislative and judicial branches. Official activities by those branches constitute “official use” as it does for other authorized recipients of CUI. While those branches often must honor the safeguard and dissemination controls required for CUI of any other recipient, marking as CUI is not itself a basis for withholding information from Congress or the Judiciary.

## **Recommendation #18 Standardize Specified Dissemination**

Agencies should work with the EA and CUI Council to standardize specified dissemination instructions. In reviewing agency requests for specified dissemination instructions, the EA should seek to harmonize instructions and thereby limit the total number of CUI specified dissemination instructions to the greatest extent possible.

## Recommendation #19 Dissemination to Congress and the Courts

Implementation guidance for the CUI framework should clarify that a CUI marking is not a basis for withholding information from Congress or the Judiciary.

### 5. Life Cycle

Life Cycle refers to the time period during which information identified as CUI would receive the safeguarding and dissemination controls of the CUI Framework. Appropriate life cycles support government transparency and ensure that resources are focused on protecting information as warranted by the level and anticipated duration of sensitivity.

The Task Force members agreed that given the volume of CUI material within the federal government, it is impracticable to implement a review process prior to decontrol. Hence, the intent is to have the life cycle established as part of the CUI designation, and be tied to either specific events or a specific timeframe.

The broad range of material covered by the CUI Framework poses difficult life cycle challenges. The Task Force believes CUI should be decontrolled as soon as it no longer warrants the safeguarding or dissemination controls of the CUI Framework. While in some cases this time frame would be foreseeable and reasonably short, in other instances, such as situations in which the Privacy Act or the Health Insurance Portability and Accountability Act apply, the timelines for protection may span the life of the protected individual, or longer.

Agency officials who recommend designation of CUI are in the best position to judge how long CUI protection should be required. The designation decisions should therefore address decontrol. Each CUI designation recommendation should specify either the passage of a certain period of time or an event certain (for example, the death of the individuals named, conclusion of prosecution and expiration of appeal rights, etc.) after which the document would be decontrolled and lose its status as CUI.

The Task Force believes that no document should remain subject to CUI controls indefinitely, and identified the requirement for a default lifecycle for any situation where no other life cycle is identifiable. Recognizing that the selection of such a generally applicable time period is both necessary and somewhat arbitrary, the Task Force considered the recommendations of both The Constitution Project (2-10 years)<sup>30</sup> and OMB Watch (not more than 5 years).<sup>31</sup> The Task Force considered these recommendations in light of the anticipated breadth of CUI designations, the significant administrative burden resulting from an overly aggressive decontrol cycle, and the enhanced transparency afforded by separating CUI status from releasability decisions (described below), and concluded that in circumstances where CUI lifecycle is otherwise

---

<sup>30</sup> The Constitution Project, *Reining in Excessive Secrecy: Recommendations for the Reform of the Classification and Controlled Unclassified Information Systems* (2009) at 9, available at <http://www.constitutionproject.org/manage/file/178.pdf>

<sup>31</sup> OMB Watch, *Controlled Unclassified Information: Recommendations for Information Control Reform* (2009) at 10, available at <http://www.ombwatch.org/files/info/2009cuipt.pdf>

undetermined, decontrol should occur 10 years following CUI identification. Any CUI whose decontrol is other than 10 years after identification should be clearly marked with the date or event certain upon which decontrol would take place.

The Task Force recognizes that decontrol of CUI is distinct from release of CUI, and that mandatory, pre-release review procedures, particularly when conducted following decontrol, facilitate coordination with the document's originator and awareness of any enduring requirement for control. At no time, pre- or post-decontrol, is a CUI marking itself determinative of whether it may be released. Similarly, the CUI Framework should not impact destruction timelines established through statute, regulation, or records management policy.

### ***Recommendation #20 Clarify Decontrol***

“Decontrol” should be identified as the act of removing information previously designated as CUI from the CUI Framework, and it should be made clear that while public release of CUI should be preceded by the CUI's decontrol, decontrol is not itself authorization for public release.

### ***Recommendation #21 Establish Life Cycle***

All CUI information should be decontrolled after ten years unless (a) the CUI designation establishes an alternative decontrol requirement by date or event, (b) the alternative decontrol appears in the controlled registry, or (c) the alternative decontrol is clearly identified on the CUI.

## **6. Exceptions**

The 2008 Memorandum lists four critical infrastructure information regimes which are specific exceptions to the CUI Framework. If the scope of CUI is expanded, as per Recommendation # 2, additional temporary exceptions may be required. To limit exceptions to those truly required, the Task Force believes it important that the EA identify specific criteria for establishing exceptions. Possible factors could include that the potential exception contains a significant amount of information not originated by the federal government and provided to the government based upon negotiated criteria that do not conform to the CUI regime, or that the provision of the information to the government is highly dependent on the existence of a trusted regime for data protection.

With respect to the four exceptions listed in the 2008 Memorandum, the relationship between the federal government and the private sector has been negotiated through public rule making. Each of these systems was negotiated and tailored to a particular community and type of information. There is significant interest in these communities that their incorporation into the Framework not negate the currently established trust. A proposal by the excepted regime program offices is to establish and implement the CUI Framework with the intention of bringing the “exceptions” into the CUI Framework once its reliability and trust are established.

The Task Force believes that the exceptions should be incorporated into the CUI Framework in a manner which, to the maximum extent possible, preserves the fundamental elements of the exceptions, and neither harms the trusted relationships nor forces the excepted regimes out of compliance with statutory requirements. As the excepted regimes approach incorporation into the CUI Framework, the Task Force believes the EA should work with the relevant agencies and program offices to amend regulations and, if necessary, with Congress to amend relevant statutes. Incorporating the exceptions into the Framework is not intended to negate established FOIA exemptions.

Any new exceptions should be considered in light of the ability to render them compliant either with existing CUI standards for safeguarding and dissemination or standards for the classification of information for national security or other authorized purposes.

### ***Recommendation #22 Establish Exception Process***

In addition to the four existing exceptions within the Presidential guidance on CUI, a process should be developed by the EA, in coordination with the CUI Council, to develop a means of evaluating whether additional categories of information that are covered by the expanded scope of CUI should be treated as temporary exceptions.

### ***Recommendation #23 Delay in Incorporation of Exceptions into the CUI Framework***

The CUI Framework should be established, running, and proven, prior to incorporation of the exceptions into the Framework.

### ***Recommendation #24 Amending Regulations or Statutes***

The EA should work with the agencies and program offices administering excepted regimes to amend relevant regulations and, if necessary, with Congress to amend relevant statutes, as the excepted regimes are incorporated into the CUI Framework.

## **7. Training**

Effective implementation of the CUI Framework requires changing the way unclassified information protection and sharing is commonly understood. A dedicated, centralized training program is critical to that effort. CUI training is required at various levels of instruction, based upon agency mission and employee duties and seniority. Baseline training should be established by the EA, and agencies should coordinate development of intermediate and advanced level training with the EA. 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. Additionally, the EA should provide training to the senior officials responsible for CUI designation and agency CUI program management.

### ***Recommendation #25 Establish Training***

The EA should establish a baseline training program sufficient to educate federal employees on the key principles underlying the CUI Framework, including the importance of government transparency and public trust in government. 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. Basic CUI training should be the minimum requirement for an employee to be authorized to identify or disseminate CUI. Additionally, to promote consistency across the Executive Branch the EA should provide training directly to the senior officials responsible for CUI designation and agency CUI program management.

## **8. Incentives and Accountability**

The Task Force believes that getting CUI designation and identification decisions right the first time is as important as ensuring compliance with CUI safeguards and dissemination controls. Like recent efforts with regard to the ISE, compliance with CUI policies should be viewed as routine elements of job performance and considered in employee evaluation, promotion, or award decisions. Moreover, administrative or other appropriate sanctions should be available for repeated non-compliance with CUI policies, or with CUI safeguard or dissemination control requirements.

### ***Recommendation #26 Incentives***

Agencies should consider employee performance under the CUI Framework in evaluation, promotion, and award decisions.

### ***Recommendation #27 Accountability and Sanctions***

Agencies should be authorized to impose administrative sanctions for repeated non-compliance with CUI policies or with CUI safeguard or dissemination control requirements.

## **9. Standardization, Oversight, and Dispute Resolution**

A simple, concise, and standardized CUI Framework, with effective centralized governance and oversight, has the best chance not only for the widest acceptance within the federal government, but for broad adaptation throughout our State, local, tribal, and private sector partner communities.

The Task Force believes it is critical that the CUI Framework bring standardization to current SBU processes to reduce inconsistency and a tendency toward over-protection of

information. To accomplish this goal, the Task Force determined that the EA should be appropriately empowered to harmonize and standardize designations across agencies.

The Task Force considers that oversight should begin within the agency, based on procedures to be set out by the agency head. Agencies should establish an effective internal oversight approach, either as part of or parallel with the CUI program.

The EA should maintain oversight authority and the ability to perform on-site reviews of agency CUI programs to support the implementation of an effective Framework across government, and to require of each agency any reports, information, and other cooperation that may be necessary to fulfill its responsibilities. In addition, each agency and the EA should also establish a mechanism for addressing challenges to CUI designation and identification by authorized holders of the information.

CUI dispute resolution requires a balanced approach. The goal is to empower the EA to implement and manage the CUI Framework while recognizing the authority of the agencies to execute their missions. CUI is likely to be fully embedded throughout mission execution, and agencies require a means of assuring that decisions within the CUI Framework do not improperly impact mission execution.

The Task Force also recognizes the significant costs imposed on private entities doing business with the federal government in order to comply with multiple, inconsistent SBU regimes. The Task Force believes the obligation under federal contracts to handle CUI information should be clear, consistent, and reflected in a single Federal Acquisition Regulation (FAR) provision that addresses the handling of CUI across the federal government. The language of this provision should be mirrored in agency-level acquisition regulations and guidance.

### ***Recommendation #28 Internal Oversight***

Each agency should identify an internal oversight program to assure the effective implementation of the CUI Framework within the agency.

### ***Recommendation #29 Challenges to Designation and Identification***

Each agency head or senior official should establish a mechanism for addressing challenges to CUI designation and identification, to include appeals to the CUI Council. The EA should establish a mechanism by which the CUI Council would address appeals of agency challenges as well as other interagency disputes based upon CUI designation or identification.

## **Recommendation #30 Federal Acquisition Guidance**

The Federal Acquisition Regulations should be revised to reflect one provision or clause that addresses compliance with the CUI Framework by private entities seeking to do business with the federal government. This provision or clause should be mirrored in agency specific acquisition regulations or guidance.

### **10. Implementation Timeline and Resources**

Full implementation of the CUI Framework requires significant resources, especially with respect to IT safeguards. Previously released safeguarding guidance required Federal IT systems to make use of encryption, two-factor authentication for remote access, and other secure system and data access procedures. Many agencies are still developing procedures to meet these requirements. Accelerating the implementation of the safeguarding requirements could impact resource constraints at certain agencies.

Raising the level of IT safeguards, however, was not among the factors mandating the replacement of the existing 107 disparate SBU regimes, the development of the CUI Framework, or the expansion of the CUI Framework beyond its current scope. Those actions were mandated by the need to bring standardization, ease information sharing, and increase government transparency to the world of SBU information. If, in the alternative, implementation focuses on the core requirements of training, marking and oversight, while still requiring an extraordinary effort, the mandates of the CUI Framework can likely be achieved for a fraction of the cost anticipated by current planning.

Therefore, to see more immediate improvements without requiring an inordinate and potentially impossible investment, the Task Force believes that implementation should begin with the foundational aspects of the CUI Framework – training, marking, and oversight, while the EA works to identify or develop appropriate IT safeguarding requirements and capabilities. Automated tools could greatly ease the burden of identifying and marking efforts by providing users with clear choices – such as are available through drop-down menus, as well as aiding oversight and CUI management efforts.

Specifically, Federal agencies should prioritize:

- Establishing agency CUI Programs.
- Implementing an EA-provided training program on the fundamentals of CUI and the importance of maintaining public trust in government.
- Adopting the CUI markings and dissemination controls, while phasing out the use of existing markings.
- Deploying automated tools, such as the Intelligence Community's Classification Management Tool, on unclassified networks to enable common and consistent markings.
- Establishing oversight and reporting mechanisms.

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.

Transitioning to the new markings under CUI will largely be a matter of change management, in which agency leadership should be held accountable for implementing plans and policies to ensure the workforce transitions to CUI in a timely manner.

Implementing compliance and reporting processes and procedures would facilitate a clearer understanding of how much information is being protected, and for what reasons. Further, if made available to the public, the results of these reporting and oversight requirements will further government transparency.

### ***Recommendation #31 Phase Implementation of Training, Marking, Oversight and Reporting***

CUI implementation should prioritize:

- Establishing agency CUI Programs.
- Implementing EA-provided baseline training program as well as agency developed intermediate and advanced level training,
- Adopting the CUI markings and dissemination controls, while phasing out the use of existing markings.
- Implementing automated tools on unclassified networks to enable common and consistent markings.
- Establishing oversight and reporting mechanisms.

### ***Recommendation #32 Phase Implementation of Technical Safeguards***

Information Technology safeguards should be phased into the CUI Framework pursuant to timelines established by the EA when, in coordination with the CIO Council, the EA determines that technical safeguards will enhance, and not degrade, the effectiveness of the CUI Framework.

### ***Recommendation #33 Marking Initiation***

Marking in accordance with the CUI Framework should begin as directed by the EA. No CUI marking should be done prior thereto. Material previously developed and disseminated, printed, or otherwise memorialized should not be remarked. Information that continues to be disseminated should be remarked at agency discretion.

### ***Recommendation #34 Ensure Adequate Resourcing of Executive Agent***

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.

### ***Recommendation #35 Synchronize CUI Implementation with Government Processes and Cycles***

CUI implementation should be incorporated into the appropriate policy, budgetary, and administrative cycles so that the implementation of the CUI Framework better aligns with current agency and Federal government business practices.

### ***Recommendation #36 Impact of CUI on the Federal Enterprise Architecture***

Members of the CUI Council should solicit feedback from their agency CIOs on how the CUI Framework can most effectively be incorporated into the Federal Enterprise Architecture (“FEA”), reflecting priorities which support business processes to enhance efficiency in implementation. This feedback should then be reviewed with OMB, and based on OMB feedback, the CUI Council – through agency CIOs and other appropriate policy officials – should work to develop specific input to the FEA within established guidance for review and possible incorporation into government-wide FEA guidance.

### ***Recommendation #37 Incorporate CUI into Federal Grant Guidance***

Federal grant guidelines for State, local and tribal government should be amended to facilitate federal grants utilization for implementation of the CUI Framework among our State, local and tribal information sharing partners, as appropriate.

## **3.3 Measures to Track Progress in Implementation of CUI**

The 2009 Memorandum identifies three presumptive goals for implementation of the Framework:

- standardization;
- information sharing; and
- government transparency

Implementation of CUI will require significant cultural changes, including a more proactive balancing of security and openness. Given that an overemphasis of either security or openness will jeopardize these goals, ongoing assessment should be a prominent part of the implementation process.

The Task Force identified three stages of CUI Framework implementation:

- Planning – the Framework is developed, tested, and put in place, including EA and agency policies, the CUI Registry, and the CUI training program;
- Transition – agencies modify existing practices to conform to the Framework; and
- Sustainment – agencies consistently apply the Framework as standard practice

The measures used to track progress will change based on the stage of implementation, but they will always support the overarching goals established by the 2009 Memorandum. In order to fully assess the Framework, the status quo must be understood and documented. It will be critical to perform baseline analysis and develop ongoing measurement programs that fully meet these complex goals. In addition, annual reporting will allow for independent public analysis as to the maintenance of the required balance, thereby improving accountability. The Task Force affirms the importance of measuring and tracking the implementation and effectiveness of the Framework.

#### ***Recommendation #38 Annual Report of the Executive Agent***

The EA should publish an annual report to the President, that is also made available to the Congress and the public, that provides the status of CUI implementation to include performance measurement data developed pursuant to Recommendation #40, and other information as deemed appropriate by the EA in consultation with the CUI Council.

#### ***Recommendation #39 Establish a Baseline Measurement of Current SBU Efforts***

Based on the system established above, the EA should immediately undertake to establish a baseline measurement of SBU activity to support future implementation and assessment efforts.

#### ***Recommendation #40 Measure Implementation***

The EA, in coordination with OMB (including the Chief Performance Officer and the Resource Management Office) and appropriate expert support, should develop a system to measure the implementation of CUI that addresses the various phases of implementation and is effectively tied to the federal budget cycle.

## Part 4. Conclusion

Through its 90-day study, the CUI Task Force concluded that within the Executive Branch, information sharing and transparency suffer from inconsistency in SBU policies, uncertainty in interagency settings as to what policies apply to SBU information, and the inconsistent application of even similar policies across agencies. The general lack of effective, standardized training and oversight at many agencies results in a tendency to over-protect information.

The Controlled Unclassified Information (CUI) Framework provided a good start toward addressing these deficiencies, but was intended to do so only with regard to terrorism-related information. The Task Force has concluded that a single, standardized framework for marking, safeguarding, and disseminating all Executive Branch SBU is required to further the goals of standardization, information sharing, and government transparency.

The Task Force recommendations are intended to overlay, and in some cases modify, the CUI Framework established by the 2008 Memorandum. Building upon that Framework, the Task Force has proposed 40 Recommendations, including simplifying the definition of CUI; expanding the scope of the CUI Framework; clarifying that limits of CUI markings – such as with regard to releases under FOIA or to Congress; and phasing implementation of the expanded scope of CUI to ensure no disruption to agencies' mission performance or the security of information.



# APPENDIX 1

## Entities Consulted by the CUI Task Force

### Government Entities

- Controlled Unclassified Information Council
- Department of Energy, Office of Classification
- Deputy to the Director of the Federal CIO Council
  - Privacy Committee of the Federal CIO Council
- Legislative Staff Representing:
  - Senate Homeland Security and Governmental Affairs Committee
  - House Committee on Homeland Security
  - House Committee on Oversight and Government Reform
  - House Committee on the Judiciary
  - House Permanent Select Committee on Intelligence
- Excepted Regime Program Offices
- Concurrent Executive Order 12958 Review
- Office of National Drug Control Policy
- Non-ISE Agencies:
  - Department of Labor
  - Department of Agriculture
  - Department of Education
  - National Air and Space Administration
  - Consumer Product Safety Commission
  - Federal Energy Regulatory Commission
- State, Local, and Tribal Government Partners
  - International Association of Chiefs of Police
  - Garden Grove, California Police Department
  - Minnehaha County, South Dakota Sheriff's Office
  - Florida Department of Law Enforcement
  - American Probation and Parole Association

### Non-Government Entities

- Critical Infrastructure Partnership Advisory Council
- National Industrial Security Program Policy Advisory Committee
- Privacy and Open Government Advocacy Organizations
  - American Civil Liberties Union
  - The Constitution Project
  - Openthegovernment.org
  - Federation of American Scientists
  - National Security Archive
  - Public Citizen
  - OMB Watch
  - Electronic Frontier Foundation



## APPENDIX 2

### SBU Markings Currently in Use

1. SENSITIVE
2. DO NOT DISSEMINATE
3. SBU-NF
4. SBU/ NOFORN
5. UNLIMITED RIGHTS
6. GOVERNMENT PURPOSE RIGHTS
7. LIMITED RIGHTS
8. RESTRICTED RIGHTS
9. SPECIAL LICENSE RIGHTS
10. PRE-EXISTING MARKINGS
11. COMMERCIAL MARKINGS
12. CLOSE HOLD
13. RSEN
14. PREDECISIONAL PRODUCT
15. SOURCE SELECTION SENSITIVE
16. DEA SENSITIVE (DEA S)
17. SENSITIVE (SENS)
18. COPYRIGHT (DATE) (OWNER)
19. DELIBERATE PROCESS PRIVILEGE
20. RELIDO
21. EYES ONLY
22. BANK SECRECY ACT INFORMATION (BSA)
23. ACQUISITION SENSITIVE
24. ATTORNEY WORK PRODUCT
25. LIMITED ACCESS
26. RESTRICTED ACCESS
27. MEDICAL RECORDS
28. LAN INFRASTRUCTURE
29. IT SECURITY RELATED
30. LAN BACKUP SENSITIVE INFORMATION
31. SOURCE SELECTION INFORMATION
32. TRADE SECRET
33. ATTORNEY CLIENT
34. BUDGETARY INFORMATION
35. PRE-DECISIONAL,
36. FOR INTERNAL USE ONLY
37. NOT FOR DISTRIBUTION SAFEGUARDS INFORMATION (SGI)
38. AGENCY INTERNAL USE ONLY (U//AIUO)
39. TRADE SENSITIVE INFORMATION
40. SENSITIVE BUT UNCLASSIFIED (SBU)
41. HEALTH RELATED INFORMATION (EM)
42. NO DISTRIBUTION (NODIS OR ND)
43. LAW ENFORCEMENT SENSITIVE (LES)
44. EXCLUSIVE DISTRIBUTION (EXDIS OR XD)
45. FOR OFFICIAL USE ONLY (FOUO)
46. SENSITIVE STUDENT RECORDS (STR)
47. CONFIDENTIAL BUSINESS INFORMATION (CBI)
48. LIMITED OFFICIAL USE (LOU)
49. LIMITED DISTRIBUTION
50. LIMITED DISTRIBUTION (LIMDIS)
51. SENSITIVE INFORMATION (SINFO)
52. COVERED BY CONFIDENTIALITY AGREEMENT
53. ORIGINATOR CONTROLLED (ORCON)
54. CONTRACTUAL SENSITIVE INFORMATION
55. ENFORCEMENT CONFIDENTIAL INFORMATION (ECI)
56. LIMITED OFFICIAL USE INFORMATION (LOUI)
57. SUBSTANCE ABUSE RECORDS (SAB)
58. SENSITIVE SECURITY INFORMATION (SSI)
59. TITLE III COMMUNICATIONS (T3)
60. FEDERAL TAXPAYER INFORMATION
61. TECHNOLOGY TRANSFER INFORMATION
62. BOMB TECH SENSITIVE (BTS)
63. CFIOUS INFORMATION (CFIOUS)
64. RESTRICTED BY COURT ORDER (CO)
65. LIMITED USE ONLY (LUO)
66. PRIVACY ACT PROTECTED INFORMATION (PAPI)
67. PROPRIETARY INFORMATION (PROPIN)
68. CHILD VICTIM/WITNESS (CH)
69. FINANCIAL RECORDS (NON-NSL) (FR)
70. FINANCIAL RECORDS NSL (NSLF)
71. SOURCE SELECTION INFORMATION
72. LIMITED CREDIT INFORMATION NSL (NSLC)
73. SELECT AGENT SENSITIVE INFORMATION (SASI)
74. CALEA COST RECOVERY INFORMATION (CALEA)
75. INNOCENT IMAGES VISUAL INFORMATION (IIVI)
76. SENSITIVE TREATY/MOU/NDA INFORMATION (STM)
77. PRIVILEGED FBI ATTORNEY CLIENT
78. OFFICIAL USE ONLY-SMALL BUSINESS
79. OFFICIAL USE ONLY-PROTECTED COOPERATIVE CENSUS CONFIDENTIAL

80. SBU-GSA-BI
81. OFFICIAL USE ONLY (OUO)
82. ATTORNEY/ CLIENT PRIVILEGED
83. GRAND JURY MATERIAL (FGJ)
84. OFFICIAL USE ONLY-APPLIED TECHNOLOGY
85. DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (DOD UCNI)
86. OFFICIAL USE ONLY-PATENT CAUTION INFORMATION
87. CONFIDENTIAL CONTRACT PROPOSAL INFORMATION (CCPI)
88. CONTROLLED NUCLEAR INFORMATION (U//DCNI OR U//ECNI)
89. CHEMICAL-TERRORISM VULNERABILITY INFORMATION (CVI)
90. NAVAL NUCLEAR PROPULSION INFORMATION (U-NNPI)
91. OFFICIAL USE ONLY-EXPORT CONTROLLED INFORMATION
92. NAVAL NUCLEAR PROPULSION INFORMATION (NOFORN)
93. SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION (SUNSI)
94. PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)
95. OFFICIAL USE ONLY - SENSITIVE INTERNAL INFORMATION
96. TELEPHONE OR ELECTRONIC COMMUNICATIONS NSL (NSLT)
97. JUVENILE - PROTECT IDENTITY IN ACCORDANCE WITH 18 USC 5031 (JI)
98. SENSITIVE INFORMATION- SPECIAL HANDLING REQUIRED
99. SENSITIVE WATER VULNERABILITY ASSESSMENT INFORMATION
100. LIMITED OFFICIAL USE-LAW ENFORCEMENT SENSITIVE (LOU-LES)
101. EXPORT CONTROLLED INFORMATION (OR MATERIAL) (ECI)
102. SENSITIVE HOMELAND SECURITY INFORMATION (SHSI)
103. OPERATIONS SECURITY PROTECTED INFORMATION (OSPI)
104. DISSEMINATION IS PROHIBITED EXCEPT AS AUTHORIZED BY AR 20-1
105. COMMUNICATION/ ATTORNEY WORK PRODUCT (PRV)
106. RESEARCH AND DEVELOPMENT AGREEMENT INFORMATION
107. INNOVATION RESEARCH INFORMATION AND SMALL BUSINESS
108. CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY ACT OF 2002 (CIPSEA)
109. WITNESS SECURITY PROGRAM - PROTECT IDENTITY IN ACCORDANCE WITH 18 USC 3521 (WS)
110. SENSITIVE DRINKING WATER RELATED INFORMATION (SDWRI)
111. CONTRACTOR ACCESS RESTRICTED INFORMATION (CARI)
112. COMPUTER SECURITY ACT SENSITIVE INFORMATION (CSASI)
113. SMALL BUSINESS INNOVATION RESEARCH (SBIR) PROGRAM
114. PERSONALLY IDENTIFIABLE INFORMATION - PRIVACY ACT OF 1974
115. PERSONNEL DATA, PRIVACY ACT OF 1974 (5 U.S.C. 552A)
116. FOR OFFICIAL USE ONLY- LAW ENFORCEMENT SENSITIVE (FOUO-LES)
117. FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

## APPENDIX 3

### Acronyms used in this report

CIO	Chief Information Officer
CUI	Controlled Unclassified Information
CVI	Chemical-Terrorism Vulnerability Information
DHS	Department of Homeland Security
DOD	Department of Defense
DOI	Department of Interior
DOJ	Department of Justice
EA	Executive Agent
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FOIA	Freedom of Information Act
FOUO	For Official Use Only (FOUO)
HHS	Department of Health and Human Service
HIPAA	Health Insurance Portability and Accountability Act
ISE	Information Sharing Environment
IT	Information Technology
LES	Law Enforcement Sensitive
NARA	National Archives and Records Administration
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PCII	Protected Critical Infrastructure Information
PM-ISE	Program Manager, Information Sharing Environment
SBU	Sensitive But Unclassified
SGI	Safeguards Information
SSI	Sensitive Security Information
USDA	Department of Agriculture





