
Controlled Unclassified Information “A Review and Revision”

By

John M. Smilek
Assistant Professor, DISAM

The very mention of the words TOP SECRET, SECRET, and CONFIDENTIAL which define the classification levels of the USG national security information, alert one to be vigilant. The Executive Order 12958 (EO 12958), as amended, establishes the Executive Branch’s Classified National Security Information Program. The EO states that, “Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation’s progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation’s security remains a priority.”¹

For most of us that work for, or with the USG, the circumstances when we will actually deal with classified information are relatively infrequent. This is not so for Controlled Unclassified Information (CUI). Many of us deal with CUI, sometimes on a daily basis, and with frequent use may come less “vigilant” habits. “The term Controlled Unclassified Information is used in the DoD to collectively describe unclassified information to which access or distribution controls have been applied pursuant to the laws and regulations of the originating country.”² If the controls are not implemented, information critical to our Nation’s security may still be compromised.

The purpose of this article is to give you a “**Review**” of CUI and explain the ongoing “**Revision**” of CUI.

Review

If CUI describes unclassified information to which access or distribution controls have been applied pursuant to laws, than what is the lawful authority? Chief among the laws that provide the legal basis for the control of CUI are the Arms Export Control Act, Export Administration Act, Freedom of Information Act and PL 98-94. The presence of access and/or distribution control markings identifies information as CUI. The primary marking for DoD is “For Official Use Only.” Some USG agencies use different markings. The standardization of markings will be part of the discussion under the REVISED portion of this article.

There are a litany of DoD regulations, directives and instructions that cover the disclosure of official information. All the documents are in the public domain and should be close at hand when questions about the control of USG information are visited. The primary documents, their number, name and primary purpose are listed below.

- DoD 5200.1-R, “*Information Security Program*,” January 14, 1997
Promotes proper and effective classification, protection and downgrading of official information requiring protection in the interest of the national security
- DoD 5400.7-R, “*Freedom of Information Act (FOIA) Program*,” September 4, 1998
Policies and responsibilities for the implementation of the DoD FOIA Program

-
- DoD Directive 5230.9, “*Clearance of DoD Information for Public Release*,” August 22, 2008
Policies and procedures for the release of information for publication or public release
 - DoD Directive 5230.24, “*Distribution Statements on Technical Documents*,” March 18, 1987
Policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations
 - DoD Directive 5230.25, “*Withholding of Unclassified Technical Data from Public Disclosure*,” November 6, 1984
Establishes policy, prescribes procedures, and assigns responsibilities for the dissemination and withholding of technical data
 - DoD Instruction 3200.14, “*Principles and Operational Parameters of the DoD Science and Technical Information Program*,” May 13, 1997
Release of DoD technical data
 - DoD Instruction 5200.39, “*Critical Program Information (CPI) Protection Within the Department of Defense*,” July 16, 2008
Protection of CPI

These documents are not meant to be a complete list of references for policies covering the disclosure of official information, but a solid base of reference.

The DoD 5400.7-R, DoD Freedom of Information Act Program (FOIA) states, “The public has a right to information concerning the activities of its Government.”³ The Regulation goes on to say, “DoD policy is to conduct its activities in an open manner and provide the public with a maximum amount of accurate and timely information concerning its activities, consistent always with the legitimate public and private interests of the American people.”⁴ The FOIA also says that USG information may not be made available if it falls within one of nine exemption categories described in the Act and the appropriate USG official determines it should be withheld from disclosure.

The list, and descriptions, of exemptions can be found in DoD 5400.7-R, Chapter 3. The first exemption deals with classified information and the other eight deal with unclassified information. A more concise list and description of the ‘unclassified information’ exemptions, extracted from the “*International Programs Security Handbook*,” is listed below.⁵

- Exemption Two: permits the withholding of information that pertains solely to the internal rules and practices of a government agency. This exemption has a high and low profile. The high profile permits the withholding of a document which, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The low profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.

-
-
- Exemption Three: permits the withholding of information that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld.
 - Exemption Four: permits withholding information such as trade secrets and commercial and financial information obtained from a company on a privileged or confidential basis which, if released, would result in competitive harm to the company.
 - Exemption Five: exempts inter- and intra-agency memoranda that are deliberative in nature. This exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
 - Exemption Six: provides for the withholding of information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of personal privacy of individuals.
 - Exemption Seven: permits withholding records or information compiled for law enforcement purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive a person of the right to a fair trial or impartial adjudication; could reasonably be expected to constitute an unwarranted invasion of personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques; or could reasonably be expected to endanger the life or physical safety of any individual.
 - Exemption Eight: permits withholding records or information contained in or relating to examination, operation or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.
 - Exemption Nine: permits withholding records or information containing geological and geophysical information and data (including maps) concerning wells.

If unclassified information is determined to qualify for an exemption under the FOIA exemptions two through nine, the DoD policy is to mark the data “FOR OFFICIAL USE ONLY (FOUO)”. Other required distribution or control markings documented in DoD Directive 5230.24 or other regulations would also apply. FOUO information must be controlled in a manner sufficient to ensure unauthorized persons do not gain access. It is usually sufficient to lock the information in a desk drawer, bookcase, filing cabinet or locking it in a room where only authorized persons may have access.

Revision

In the fall of 2007, the President of the U.S. issued “National Strategy for Information Sharing.” This document reinforces the exchange of information across all Federal Government sectors as well as with external partners. On 9 May 2008, the President released the Memorandum for the Heads of Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information. The purpose of the memo states:

(1) This memorandum (a) adopts, defines, and institutes “Controlled Unclassified Information” (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as “Sensitive But Unclassified” (SBU) in the Information Sharing Environment (ISE), and (b) establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. The memorandum’s purpose

*is to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information.*⁶

The Presidential Memorandum designates the National Archives and Records Administration (NARA) as the CUI Executive Agent to oversee and manage the implementation of the new CUI Framework. In a memorandum dated 21 May 2008, Allen Weinstein, Archivist of the U.S., officially established within the NARA the “Controlled Unclassified Information Office.” The memo goes on to say that:

*Under my direction and in accordance with the Presidential Memorandum (May 09, 2008), the Director of the Controlled Information Office shall: Develop and issue CUI policy standards and implementation guidance consistent with this memorandum, including appropriate recommendations to State, local, tribal, private sector, and foreign partner entities for implementing the CUI Framework. As appropriate, establish new safeguarding and dissemination controls, and, upon a determination that extraordinary circumstances warrant the use of additional CUI markings, authorize the use of such additional markings;*⁷

The memo lists additional actions including, but not limited to, establish and chair the CUI Council; establish, approve, and maintain safeguarding standards and dissemination instructions; establishing baseline training requirements; and advising the heads of departments and agencies on the resolution by the CUI Council of complaints and deputies among departments and agencies.⁸

A Department of Defense CUI Task Force, jointly led by the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)/DoD Chief Information Office (CIO) and the Office of the Under Secretary of Defense (OUSD) (Intelligence), was established in January 2008 to oversee development of a transition plan and identify costs associated with the implementation of the Presidential Memorandum on CUI.⁹ The Task Force has initiated a DoD CUI Transition Plan to identify specific transition activities based on a phased implementation of the CUI tasking. Phase one, in FY 10-12, will concentrate on Program and Information Technology areas to include Counterterrorism and Law Enforcement. Phase two, FY 13-15, will cover all other DoD Programs and Information Technology Areas. As the new CUI procedures are implemented, training will be required for all DoD employees. If you are a member of the Department of Defense look for more guidance on CUI over the next few years.¹⁰

It is the duty of all to control access to certain USG information critical to our Nation’s national interests. The laws, regulations, directives and instructions are available to guide us. As the new CUI framework for designating, marking, safeguarding and dissemination of information is being developed and implemented, it is up to all of us to be diligent in our efforts to put the “Control” in Controlled Unclassified Information.

About the Author

John Smilek is a DISAM Assistant Professor for the management of security assistance. He is the coordinator for the Technology Transfer and International Programs Security Requirements instruction and is the Course Manager for the CONUS Course (SAM-C). He is also an instructor in FMS logistics, acquisition and foreign policy. He has an undergraduate degree in Technical Education from the University of Akron, and a master’s degree in Management and Public Administration from Webster University.

Bibliography

1. Executive Order 13292 of March 23, 2003. Further Amendment to Executive order 12958, as amended, Classified National Security Information.

-
-
2. *International Programs Security Handbook C4.B, Controlled Unclassified Information and Foreign Government Information*, Jan 1, 2006.
 3. DoD 5400.7-R, *DoD Freedom of Information Act Program*, C1.3.1.1.
 4. Ibid.
 5. *International Programs Security Handbook C4.B2*.
 6. Bush, George W. "Designation and Sharing of Controlled Unclassified Information." *Memorandum For The Heads of Executive Departments and Agencies*, May 9, 2008.
 7. Weinstein, Allen. "Establishment of the Controlled Unclassified Information Office." *Memorandum*, May 21, 2008.
 8. Ibid.
 9. Grimes, John G., Clapper, James R. Jr. "White House Approval of Controlled Unclassified Information (CUI) Policy Framework." *Memorandum*, July 21, 2008.
 10. Ibid.