Description of document:	Department of Education (ED) Directive on Controlled Unclassified Information (CUI) 2019
Requested date:	28-June-2021
Release date:	06-July-2021
Posted date:	06-May-2024
Source of document:	FOIA Request U.S. Department of Education Office of the Executive Secretariat FOIA Service Center 400 Maryland Avenue, SW, LBJ 7W106A Washington, DC 20202-4536 ATTN: FOIA Public Liaison Fax: (202) 401-0920 Freedom of Information Act Public Access Link

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE SECRETARY

FOIA Service Center

July 6, 2021

RE: FOIA Request No. 21-02016-F

This letter is a final response to your request for information pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, dated June 28, 2021 and received in this office on June 28, 2021. Your request was forwarded to the Office of the Chief Information Officer (OCIO) to search for documents that may be responsive to your request.

You requested the following: A copy of the Department of Education CUI Policy document. CUI stands for Controlled Unclassified Information. This document was completed in late 2020 or early 2021.

Available for Public Access Link (PAL) download are 57 pages of fully releasable documents responsive to your request. The documents are as follows:

- Controlled Unclassified Information Program.

You can access your PAL account at this link: https://foiaxpress.pal.ed.gov/app/PalLogin.aspx

Provisions of the FOIA allow us to recover the costs pertaining to your request. The Department has concluded that you fall within the category of Other. However, the Department has provided you with this information at no charge. The Department's release of this information at no cost does not constitute the grant of a fee waiver and does not infer or imply that you will be granted a fee waiver for future requests made under FOIA to the Department. Because we were able to locate and process these documents at minimal costs, they are provided to you at no cost.

You have the right to seek further assistance from the Department's FOIA Public Liaison, Robert Wehausen. The Department's FOIA Public Liaison can be reached by email at robert.wehausen@ed.gov; by phone at 202-205-0733; by fax at 202-401-0920; or by mail at Office of the Executive Secretariat, U.S. Department of Education, 400 Maryland Ave., SW, 7C132, Washington, DC 20202-4500, Attn: FOIA Public Liaison.

If you have any questions, please contact the FSC at (202) 401-8365 or EDFOIAMANAGER@ed.gov.

Sincerely,

DeShawn Middleton

DeShawn Middleton
Government Information Specialist
Office of the Executive Secretariat

Enclosure

ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

Distribution:
All Department of Education
Employees and Contractors

Signed by: Denise L. Carter
Acting Assistant Secretary
Office of Finance and Operations

Controlled Unclassified Information Program

Table of Contents

This is a new directive.

For technical questions regarding this Administrative Communication System (ACS) document, please contact Jason Lautenbacher at Jason.lautenbacher@ed.gov or via telephone at (202) 245-7303.

This ACS Departmental Directive supersedes ACS Departmental OCIO-15, "Handbook for Protection of Sensitive but Unclassified Information," dated 03/30/2007.

I. Purpose

This Administrative Communications System (ACS) Directive (Directive) implements Executive Order 13556 and 32 CFR part 2002, both titled Controlled Unclassified Information (CUI). These authorities institute national policy on the handling, safeguarding, and control of information the executive branch agencies create or possess that a law, regulation, or Government-wide policy requires or specifically permits an agency to handle by means of safeguarding or dissemination controls. Classified National Security Information (CNSI) is not included in the CUI Program. This Directive creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the Department of Education, its officers, employees, or agents, or any other person.

II. Applicability

This Directive applies to all Department of Education (Department or ED) principal offices and to all ED covered individuals/entities. For purposes of this Directive, ED covered individuals/entities include ED employees, contractors (on-site and off-site), who agree to adhere to the terms and conditions of this Directive, and affiliated parties such as consultants, researchers, organizations, and State, local, Tribal, and private sector partners with whom ED shares CUI and who agree to adhere to the terms and conditions of this Directive.

III. Limitations on Applicability of this Directive

Any CUI requirements contained in this Directive or ED principal offices' policies that are not supported by law, regulation, or Government-wide policy may not be applied to outside entities, unless the law, regulation, or Government-wide policy permits ED to impose such requirements. When entering into agreements, ED may not include additional requirements or restrictions on handling CUI other than those permitted in the CUI Program. 32 CFR part 2002 overrides any requirements set forth in this Directive or ED principal offices' policies when they conflict.

IV. References*

A. Executive Order 13556, Controlled Unclassified Information, dated November 4, 2010, as published in the Federal Register on November 9, 2010 (75 FR 68675). (https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information)

* NIST publications are accessible at http://csrc.nist.gov/publications; Code of Federal Regulations are accessible at http://www.ecfr.gov/cgi-bin/text-idx?tpl=%2Findex.tpl; and Executive Orders are accessible at https://www.federalregister.gov/presidential-documents/executive-orders.

B. 32 CFR part 2002, Controlled Unclassified Information, issued September 14, 2016. (https://www.govinfo.gov/content/pkg/FR-2016-09-14/pdf/2016-21665.pdf)

C. CUI Notice 2017-01, Implementation Recommendations for the Controlled Unclassified Information Program, issued June 12, 2017, (https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/2017-cui-notice-2017-01-implementation-recommendations.pdf)

D. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

E. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf)

F. FIPS Publication 140-2, Security Requirements for Cryptographic Modules, issued May 25, 2001 (Change Notice 2, December 3, 2002). (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf)

G. NIST Special Publication (SP) 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (updated January 22, 2015). (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

H. NIST SP 800-88, Rev. 1, Guidelines for Media Sanitization, December 2014.

I. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, June 2018. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf)

J. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 20, 2018. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf)

K. Federal Acquisition Regulation (FAR). The FAR is codified at 48 CFR Chapter 1. (https://www.acquisition.gov/?q=browsefar). FAR 48 CFR § 52.204-21 includes a clause regarding basic safeguarding of covered contractor information systems. (https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems).

L. Department of Education Acquisition Regulation, 48 CFR Chapter 34. (https://www.acquisition.gov/?q=browsefar).

M. Federal Information Security Management Act (FISMA) of 2002 (Title III of Pub. L. No. 107-347 (2002), (http://csrc.nist.gov/).

N. Federal Information Security Modernization Act (FISMA) of 2014 (Pub. L. No. 113-283 (2014)), available at (https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf)).

O. Federal Information Technology Acquisition Reform Act (FITARA) (Division A, Title VIII, Subtitle D of Pub. L. No. 113–291 (2014)). (https://www.congress.gov/).

P. Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 28, 2016, which may be found at (https://obamawhitehouse.archives.gov/omb//).

Q. National Archives and Records Administration (NARA) Bulletin 2013-02 (2013), Guidance on a New Approach to Managing Email Records (https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html).

R. NARA Controlled Unclassified Information (CUI) Registry, Limited Dissemination Controls, which may be found at (https://www.archives.gov/cui/registry/limited-dissemination).

S. NARA Controlled Unclassified Information (CUI) Registry, Marking Guide, which may be found at (https://www.archives.gov/files/cui/documents/into-to-marking-ppt-201808.pdf).

T. NARA Controlled Unclassified Information (CUI) Registry, which may be found at (https://www.archives.gov/cui/registry/category-list).

V. Cancellations

This Directive supersedes the ACS Departmental Handbook OCIO-15 "Handbook for Protection of Sensitive But Unclassified Information" dated March 30, 2007.

VI. Cross References

Where applicable sections of this Directive will provide a cross reference to the corresponding section of 32 CFR part 2002 and will be indicated by "[CFR § 2002.xx]." Questions regarding this Directive may be referred to the ED CUI Program Manager within the Office of the Chief Information Officer (OCIO), Information Technology Program Services Branch.

VII. Definitions

A. Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. 32 CFR § 2002.4(h).

B. Appendix B of this Directive and 32 CFR § 2002.4 contain additional definitions applicable to this Directive and the CUI Program.

VIII. Background

In November 2010, the President issued Executive Order 13556, Controlled Unclassified Information, 75 FR 68675 (November 4, 2010) (Order) to establish a program for managing Controlled Unclassified Information (CUI) to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls." Prior to that time, more than 100 different markings for such information existed across the executive branch. This *ad hoc*, agency-specific approach created inefficiency and confusion, led to a patchwork system that failed to adequately safeguard information requiring protection, and unnecessarily restricted information-sharing.

As a result, the Order established the CUI Program to standardize the way the executive branch handles information that requires safeguarding or dissemination controls (excluding information that is classified under Executive Order 13526, Classified National Security Information, 75 FR 707 [December 29, 2009], or any predecessor or successor executive order; or the Atomic Energy Act of 1954 [42 U.S.C. § 2011, *et seq.*] as amended.)

The National Archives and Records Administration (NARA) is the CUI Executive Agent (EA) responsible for developing policy and providing oversight for the CUI Program. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

The NARA CUI EA has established a CUI Registry[1] that serves as the authoritative reference for all CUI category markings.

IX. Policy

ED shall protect all CUI in accordance with national directives, applicable laws, regulations, Department policies, and the Order; ensure that contract employees and other ED covered individuals/entities exercise the same level of care in protecting CUI as ED is required to; and remove any CUI-mandated controls on

[1] "CUI Registry". The full URL is http://www.archives.gov/cui/registry/category-list.html.

the information once it is decontrolled.[2] Questions about whether information should be designated CUI should be directed to the ED CUI Program Manager for clarification.

There shall be a period of time allowed for conversion to the CUI Program. The date of full implementation of the program will be announced by the ED CUI Senior Agency Official (SAO). The implementation of the ED CUI Program will be conducted in phases beginning with policy adoption followed by training. During this phased implementation legacy markings and safeguarding practices will remain in effect. After the full implementation of the ED CUI program, all ED covered individuals/entities shall discontinue the use of legacy[3] or other markings and safeguarding practices not permitted by the CUI Program, and use only the CUI Program markings listed in Appendix C and the CUI Registry.

X. Appendices

A. Appendix A, Acronyms.

B. Appendix B, Definitions.

C. Appendix C, CUI Marking.

D. Appendix D, Examples.

E. Appendix E, Multiple Category and Banner Markings: Basic & Specified.

XI. Responsibilities

A. **The Chief Information Officer (CIO)** on behalf of the Secretary of Education shall:

1. Ensure Departmental senior leadership support;

2. Make adequate resources available to implement, manage, and comply with the requirements of the Order and 32 CFR part 2002 (Controlled Unclassified Information (CUI));

---

[2] Removal of CUI controls does not constitute authorization to release the information. For instance, Freedom of Information Act (FOIA) and the Privacy Act of 1974, as amended (Privacy Act) considerations remain in effect regarding the release of government information. Decontrolling occurs when an authorized holder, consistent with 32 CFR §§ 2002.4(s) and 2002.18 and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action.

[3] Legacy-marked information contains markings that were in use before the advent of the CUI Program, e.g., For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) (e.g., Sensitive Security Information [SSI]), and some are discontinued (e.g., FOUO and SBU).

3. Ensure ED senior leadership make adequate resources available to implement, manage, and comply with the Department's CUI Program;

4. Advise the NARA CUI EA of whom ED designates as the CUI SAO responsible for oversight of the ED's CUI Program implementation, compliance, and management, and include the CUI SAO in all contact listings;

5. Advise the NARA CUI EA of any changes to the designated CUI SAO;

6. Approve Departmental policies as needed to implement the Department's CUI Program consistently with 32 CFR § 2002.8(b)(3); and

7. Establish and maintain a self-inspection program to ensure the Department complies with the principles and requirements of Executive Order 13556 dated November 4, 2010, 32 CFR part 2002, and the CUI Registry.

B. **The ED Information Technology Program Services Director** is the SAO for CUI with duties and responsibilities as follows:

1. Direct and oversee the Department's CUI Program;

2. Make requests for adequate resources to implement, manage, and comply with the Department's CUI Program;

3. Designate a CUI Program Manager;

4. Ensure the Department has CUI implementing policies and plans as needed;

5. Develop new and/or execute upon current Department-wide policies and procedures necessary to manage a CUI program that complies with the Order and 32 CFR part 2002;

6. Implement an education and training program pursuant to 32 CFR § 2002.30 to include monitoring for compliance with training requirements;

7. Ensure the training and education program for both basic and specified categories of CUI includes sufficient information that allows all ED covered individuals/entities to understand and carry out their obligations with respect to designating, marking, safeguarding, storing, transmitting, transporting, decontrolling, and destroying CUI materials;

8. Upon request of the NARA CUI EA provide updates of the Department's CUI implementation efforts as part of the annual report to NARA;

9. Assist in and respond to audits conducted by the NARA CUI EA;

10. Include a description of all waivers granted in Part C 7a of the annual report to the NARA CUI EA, along with the rationale for each waiver and the alternative steps being taken to ensure sufficient protection of CUI within the Department (see section XXXIII below);

11. Develop and implement the Department's self-inspection program;

12. Establish a process to accept and manage challenges to CUI status (including improper or absence of marking) in accordance with existing processes based in laws, regulations, and Government-wide policies;

13. Establish processes and criteria for reporting and investigating misuse of CUI;

14. Notify authorized recipients and the public of any waivers the Department grants (unless notice is otherwise prohibited by law, regulation, and Government-wide policy) and separately notify the NARA CUI EA;

15. Submit to the NARA CUI EA any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that the Department proposes to use to designate unclassified information for safeguarding or dissemination controls;

16. Coordinate with the NARA CUI EA, as appropriate, any proposed law, regulation, or Government-wide policy that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI;

17. Document a description of all existing waivers in the annual report to the NARA CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps the Department is taking to ensure sufficient protection of CUI within the Department;

18. Establish processes for handling CUI decontrol requests submitted by authorized holders;

19. Establish a mechanism by which authorized holders (both inside and outside the Department) can contact a designated Department representative for instructions when they receive unmarked or improperly marked information the Department designated as CUI;

20. Ensure IT and information contracts and other applicable procurements documents include relevant security and privacy language to protect the

confidentiality, integrity, and availability of ED systems and information; and

21. Assist in determining the applicability to solicitations and contracts of the clauses in the Federal Acquisition Regulation that must be inserted when the design, development, or operation of a system of records on individuals is required to accomplish a function of the Department's and/or other privacy-related clauses in the Department of Education Acquisition Regulation (EDAR) at 48 CFR Chapter 34.

C. The **CUI Program Manager** shall:

1. Implement the CUI Program within ED as described in this Directive, the Order, and in 32 CFR part 2002;

2. Serve as the Department's official representative to the NARA CUI EA on the Department's day-to-day CUI Program operations, both within ED and in interagency contexts;

3. Serve as the Department's official representative on the Interagency CUI Advisory Council to advise the NARA CUI EA on the development and issuance of policy and implementation guidance for the CUI Program;

4. Serve as the Department's most senior Subject Matter Expert (SME) in CUI, advising the ED principal offices on their CUI programs to ensure CUI operations comply with all applicable requirements;

5. Oversee the implementation and management of the CUI Program among the ED principal offices;

6. Lead an ED CUI Working Group of representatives from each principal office to develop and guide the implementation and continuing management of the Department's CUI Program;

7. Convey requirements for training and reporting to ED principal offices; consolidate status reports from the principal offices and forward Departmental reports to the NARA CUI EA;

8. In consultation with the ED principal offices, develop a basic CUI training program for the Department and assist the principal offices with developing additional training that is particular to each of their offices;

9. In consultation with the ED principal offices, develop a specialized training program to support their efficient and effective implementation of CUI in their offices; and

10. Maintain an internal website or SharePoint site available for all employees to use that contains information about the CUI Program, with a section for each principal office to list their frequently-encountered CUI categories and special instructions.

D. The Head of an **ED Principal Office** shall:

1. Appoint a senior employee (GS-14 or above) and an alternate as CUI Points of Contact (POC) to assist in implementing and managing the CUI Program within their offices, and to represent their offices on the ED CUI Working Group;

2. Promptly notify the ED CUI Program Manager of any change to the designated CUI POC for their office;

3. Ensure CUI policies, procedures, and practices within their office comply with ED's CUI requirements as specified in this Directive; and

4. Make adequate resources available to implement, manage, and comply with the CUI Program.

E. The **Director of Information Technology Services (ITS)** shall:

1. Develop a strategy or a plan to modify all information technology systems that contain, or that are used to process CUI, to ensure these systems meet the Federal baseline control of moderate confidentiality;

2. Issue guidance regarding acceptable methods of protecting CUI within IT systems (including email) and transmitting CUI from ED email systems; and

3. Issue guidance regarding acceptable methods of protecting CUI on public-facing websites and in cloud based systems.

F. The **General Counsel**, or **designee** shall:

Provide advice and legal counsel regarding the requirements of the Order and 32 CFR part 2002 and administration of the Department's CUI Program.

G. The **Counsel to the Inspector General**, or **designee** shall:

When appropriate to preserve the independence of the Office of Inspector General (OIG), provide such advice and legal counsel to the Inspector General and the OIG regarding the requirements of the Order and 32 CFR part 2002 and administration of the Department's CUI Program.

H. **Designated CUI Points of Contact** and **alternates** shall:

1. Complete all training as required to ensure their full capability to function as the CUI POC for their principal office;

2. Provide oversight and report compliance with this Directive, annually to the Information Technology Program Services (ITPS) CUI Program Management Office (PMO);

3. Serve as their principal office's CUI SME, responding to most inquiries from their principal office and consulting with ED's CUI Program Manager regarding inquiries that are beyond their expertise;

4. Serve on the ED CUI Working Group as their principal office's representative to assist in developing, implementing, and managing CUI policy and programs throughout the Department;

5. With assistance from the ED CUI Program Manager, modify ED's CUI materials to address particular needs relevant to their principal office business functions, e.g., identify CUI categories to nominate for inclusion in CUI Registry, modify training materials and job aids, update ED policies and procedures;

6. Maintain their principal office section of the ED CUI website or SharePoint site with current information;

7. Ensure all ED covered individuals/entities (employees, contract employees, and other associated covered individuals/entities) within their principal office complete CUI training in accordance with the requirements of this Directive, and report the progress of training to the ED CUI Program Manager;

8. Conduct annual self-inspections of their program to reflect the progress of implementation and report the results of those self-inspections to the ED CUI Program Manager;

9. Provide input from their principal office on all other reporting requirements to the ED CUI Program Manager, to enable a Departmental response to the NARA CUI EA;

10. Report instances of potential CUI violation or infractions to the ED CUI Program Manager; and

11. Keep track of violations for reporting purposes.

I. The **Contracting Officers (COs), Contracting Officer's Representatives (CORs)** and **Grant Managers** shall:

1. Ensure the applicable Federal and Departmental CUI security clauses are included in their assigned contracts. CORs shall also ensure contractors are aware of and understand the CUI security clauses in their assigned contracts;

2. Ensure the applicable Federal and Departmental CUI security clauses are included in their assigned contracts. Grant Managers shall also ensure grantees are aware of and understand the CUI security clauses in their grant awards;

3. Include in all contracts which may involve CUI a clause requiring that the contractor comply with NIST SP 800-171[4] for any non-Federal computer system they operate that contains CUI. See 32 CFR § 2002.14(h) (2) for more information; and

4. Confer with the System Owner, Information System Security Officer (ISSO), Information Technology Program Services (ITPS), Office of the Chief Information Security Officer (CISO), and Privacy Safeguard Team when developing a contract involving other types of IT procurements to make sure all applicable security and privacy language is included.

J. The **Supervisors** and **Managers** shall:

1. As needed, review and ensure that all CUI products are properly marked in accordance with this policy;

2. Annually verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access); and

3. Ensure that all covered individuals under their supervision receive CUI training in accordance with the requirements of this Directive.

K. **ED covered individuals/entities, including but not limited to ED employees, contractors**, and **affiliated parties** shall:

1. Complete all CUI training within the required timeframes.[5]

---

[4] National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations.

[5] Only covered individuals/entities who are highly unlikely to encounter sensitive Government information in their duties are exempt from the training requirement. These covered individuals/entities could include service and maintenance personnel and contractors, food service workers, parking attendants, etc.

2. Manage, mark, and protect CUI in accordance with this Directive.

3. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), or Sensitive but Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the information leaves the Department. Only markings that are contained in the NARA CUI Registry[6] may be used to annotate CUI. See section XVIII E. below.

4. Report incidents of CUI misuse, in accordance with the procedures set forth in XXXVIII below, as needed.

5. Contact the CUI PMO to request new CUI categories or to report missing or mislabeled CUI categories.

XII. Key Elements of the CUI Program

A. The CUI Registry [32 CFR § 2002.10] is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the NARA CUI EA. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes applicable decontrolling procedures and policy and guidance on handling procedures for unclassified information that requires safeguarding or dissemination controls. The CUI Registry is available at https://www.archives.gov/cui/registry/category-list.

B. CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does NOT set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry. CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information.

C. ED CUI categories. [32 CFR § 2002.12]

1. CUI categories are those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise

[6] The NARA CUI Registry is the authoritative source for all markings that may be used to identify sensitive unclassified information.

safeguarding or dissemination controls, and which the NARA CUI EA has approved and listed in the CUI Registry. The Order and the CUI regulations do not allow the Department to implement safeguarding or dissemination controls for any unclassified information other than those for CUI.

2. ED covered individuals/entities may use only those categories approved by the NARA CUI EA and published in the CUI Registry to designate information as CUI. ED covered individuals/entities should contact the CUI PMO to request new CUI categories, or to report missing or mislabeled categories. The CUI PMO will contact the NARA CUI Program Office for clarification and assistance.

XIII. Safeguarding [§ 2002.14]

A. The objective of safeguarding is to prevent the disclosure of CUI to unauthorized individuals.

B. Unless different protection is specified in the CUI Registry (see subparagraph C below), CUI that is not within Federal information systems must be stored in a locked office, locked drawer, or locked file cabinet whenever it is left unattended. If cleaning or maintenance personnel are allowed into private offices after hours, CUI within those offices that is not within Federal information systems must be secured in a locked desk drawer or locked file cabinet.

C. Individuals working with CUI Specified categories (e.g., Sensitive Security Information - SSI) must comply with the safeguarding standards outlined in the underlying law, regulation, or Government-wide policy in addition to those described in this Directive.

D. Persons working with CUI shall be careful to not expose CUI to others who do not have a lawful Government purpose to see it. Cover sheets – Standard Form (SF) 901– may be placed on top of documents to conceal their contents from casual viewing. ED covered individuals/entities may use a cover sheet to protect CUI while they are in the vicinity of the information, but must secure CUI that is not within Federal information systems in a locked desk drawer, file cabinet, office, etc., whenever they leave the area.

E. Other Precautions.

1. ED covered individuals/entities should take necessary steps to reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed;

2. ED covered individuals/entities should keep CUI under their direct control at all times or protect it with at least one physical barrier, and take necessary steps to reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment; and

3. ED covered individuals/entities should protect the confidentiality of CUI that is processed, stored, or transmitted on Federal information systems in accordance with applicable ED policies or procedures.

    a. CUI shall not be viewed while on a public conveyance where others may be exposed to it. In hotel rooms, CUI should be kept in a locked briefcase, room safe, or in a sealed envelope in the hotel reception safe. CUI may be stored in a locked automobile only if it is in an envelope, briefcase, or otherwise covered from view. The trunk is the most secure location for storing CUI in an automobile.

    b. ED principal offices may not require more restrictive safeguarding standards for unclassified information than those described in this Directive or 32 CFR part 2002 for their contractors or other partners with whom they share CUI.

XIV. CUI Within Information Systems [§ 2002.14(g), (h)]

A. Information systems that process, store, or transmit CUI are of two different types:

1. A "Federal information system" is an information system used or operated by a Federal agency or by a contractor of an agency or other organization on behalf of an agency. (See Appendix B, Definitions, for more information about Federal information systems.) Information systems that any entity operates on behalf of ED are subject to the requirements of the CUI Program as though they are ED's systems, and ED may require these systems to meet the same requirements as our own internal systems.

2. A "non-Federal information system" is any information system that does not meet the criteria for a Federal information system. (See Appendix B, Definitions, for more information about non-Federal information systems.) Entities employing non-Federal information systems must follow the requirements of NIST SP 800-171 to protect CUI Basic, unless specific requirements are specified by law, regulation, or Government-wide policy for protecting the information's confidentiality.

B. All CUI within ED information systems shall be marked, encrypted, and where available, protected with rights-based-access-controls (rights management).

C. Non-Federal information systems containing CUI must meet NIST's "moderate" confidentiality standard as outlined in NIST SP 800-171.

D. In accordance with FIPS Publication 199, CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS Publication 199 defines security impact levels for Federal information and Federal information systems. The appropriate security requirements and controls identified in FIPS Publication 200 and NIST SP 800-53 must be applied to CUI in accordance with any risk-based tailoring decisions made. Note: FIPS Publication 200 is used for Selection of Applicable Security Controls together with NIST 800-53 Rev. 4. FIPS Publication 199 is used for Security Categorization to categorize the information system type together with NIST 800-60 Vol. 2, Rev. 1.

E. ED may increase CUI Basic's confidentiality impact level above moderate only within ED, including the confidentiality impact level of CUI Basic that resides on information systems that contractors operate on behalf of ED.

F. ED may increase CUI Basic's confidentiality impact level above moderate outside of ED only by way of an agreement with other agencies or non-executive branch entities with which the CUI is shared.

G. ED may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside ED.

H. NIST Special Publication 800-171 contains security requirements that a non-executive branch entity must meet if they receive ED CUI in their information systems but they are not using or operating those information systems on behalf of ED or another executive branch agency.

XV. Destruction [§ 2002.14(f)]

A. CUI may be destroyed:

1. When the information is no longer needed; and

2. When records disposition schedules published or approved by NARA and other applicable laws, regulations, or Government-wide policies no longer require retention.

B. Destruction of CUI, including in electronic form, must be accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI Specified [subparagraph B above] must be destroyed according to any specific directives regarding the information.

C. In accordance with Appendix A to NIST SP 800-88,[7] the destruction of paper documents containing CUI must adhere to the following:

1. Employing cross-cut shredders that produce shreds that are nominally 1 ½" X 3/8" or smaller;

2. Contracting for the services of commercial destruction companies that mix the shredded CUI material with the residue of other offices and/or organizations for recycling. These companies may employ machines that produce a larger shred size so that it is suitable for recycling. At ED and FSA headquarters buildings, CUI may be placed in special document destruction consoles and barrels located on every floor throughout the buildings. Other organizations outside of ED and FSA headquarters should evaluate the destruction vendor's process for collection, protection, transport, and destruction before issuing a contract. Questions regarding the use of commercial destruction companies may be forwarded to the Headquarters ED (CUIProgram@ED.gov) or FSA security offices;

3. Using any destruction techniques approved for classified national security information;

4. Using other means only as approved by the Headquarters ED (CUIProgram@ED.gov);

5. ED may include these destruction standards in contract specifications and grant documents, but must specify that the ED-specific destruction standards apply only to ED's CUI that the contractor handles. If the contractor also handles CUI from other agencies, the contractor must abide by 32 CFR part 2002 or the other agency's standards.

XVI. Sharing of CUI (Accessing and Disseminating) [§ 2002.16]

A. CUI may only be disseminated with others[8] provided that such sharing/dissemination:

1. Is in accordance with the laws, regulations, or Government-wide policies that established the CUI category;

---

[7] Appendix A to NIST SP 800-88 contains sanitation recommendations for CUI. Table A-1 states that paper containing CUI should be destroyed using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. However, the second paragraph of Appendix A states that methods not specified in Table A-1 or other tables for other types of media that are included in Appendix A "… may be suitable as long as they are verified and found satisfactory by the organization."

2. Furthers a lawful Government purpose;

3. Is not restricted by an authorized limited dissemination control established by the NARA CUI EA; and

4. Is not otherwise prohibited by law[9].

B. Only the limited dissemination controls published in the CUI Registry may be used to restrict the dissemination of CUI to certain individuals, agencies, or organizations. These limited dissemination controls, which are separate from any controls that a CUI Specified authority requires or permits, may only be used to further a lawful Government purpose, or if laws, regulations, or Government-wide policies require or permit their use. If ED covered individuals/entities have significant doubt about whether it is appropriate to use a limited dissemination control where ED is the authorized holder of CUI but is not the designating agency, ED covered individuals/entities should consult and follow the designating agency's policy. If, after consulting the designating agency's policy, significant doubt still remains, the limited dissemination control should not be applied.

C. CUI may be shared with entities other than executive branch agencies, under the following conditions in addition to the requirements of subparagraph (A) above:

1. When there is a reasonable expectation that all intended recipients are authorized to receive the CUI and have a basic understanding of how to handle it.

2. Whenever feasible, the ED principal office should enter into some type of formal information-sharing agreement with the recipient of the CUI. The agreement must include a requirement for the recipient to comply with the Order or any successor order, 32 CFR part 2002, and the CUI Registry. The NARA CUI regulations at 32 CFR § 2002.16(a)(7) explicitly permit CUI to be shared without a written agreement when CUI is shared with the following entities: Congress, including any committee, subcommittee, joint committee, joint subcommittee, or office thereof; a court of competent jurisdiction, or any individual or entity when directed by an order of a court of competent jurisdiction or a Federal administrative law judge (ALJ) appointed under 5 U.S.C. § 3501; the Comptroller General, in the course of performing duties of the Government Accountability Office; or

[9]ED covered individuals/entities, in consultation with the ED Privacy Office and OGC, must assess whether any privacy laws (such as the Privacy Act of 1974, as amended (5 U.S.C. § 552a), the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g), or the IES Confidentiality provisions (20 U.S.C. § 9573)), or laws with restrictions on the uses of information, such as 20 U.S.C. § 1090(a)(3)(E), prohibit the Department from disseminating or providing access to CUI.

individuals/entities, when the agency releases information to them pursuant to a Freedom of Information Act (FOIA) or Privacy Act request.

3. If ED's mission requires dissemination of CUI, but a formal agreement is not possible, ED covered individuals/entities must communicate to the recipient that ED strongly encourages the recipient to protect CUI as described in this CUI Program.

4. Foreign entity sharing [32 CFR § 2002.16(a)(5)(iii)]. When entering into information-sharing agreements or arrangements with a foreign entity, ED covered individuals/entities should encourage that entity to protect CUI in accordance with the Order or any successor order; 32 CFR part 2002; and the CUI Registry. ED covered individuals/entities are cautioned to use judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding CUI. If such agreements or arrangements include safeguarding or dissemination controls on unclassified information, only the CUI markings and controls may be used. Other markings or protective measures may not be used.

5. Information-sharing agreements that have been made prior to establishment of the CUI Program should be modified whenever feasible so they do not conflict with CUI Program requirements. [32 CFR § 2002.16(a)(5)(iv)].

6. Information sharing agreements with non-executive branch entities must include provisions that CUI be handled in accordance with the CUI Program; misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies; and any non-compliance with handling requirements must be reported to ED via protected communications described in this Directive. When ED is not the designating agency, ED covered individuals/entities must notify the designating agency. [32 CFR § 2002.16(a)(6)]

D. CUI Basic may be disseminated to persons and entities meeting the access requirements of this section. Further dissemination of CUI Basic may not be restricted without approval by NARA's CUI EA, who will publish any exceptions in the CUI Registry. Authorized recipients of CUI Basic may further disseminate the information to individuals or entities meeting and complying with the requirements of this CUI Program.

E. CUI Specified may only be disseminated to persons and entities as authorized in the underlying legislation or authority contained in the CUI Registry. Further dissemination of CUI Specified may be made to such authorized persons if not restricted by the underlying authority.

XVII. Decontrol of CUI [§ 2002.18]

A. When safeguarding or dissemination control are no longer needed, ED should, as soon as practicable, decontrol any CUI that it designates.[10] This means the information should be removed from the protection of the CUI program as soon as practicable when the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the underlying authority.

B. CUI may be decontrolled automatically upon the occurrence of one of the conditions below, or through an affirmative decision by the designator:

1. When laws, regulations or Government-wide policies no longer require its control as CUI and the authorized holder[11] has the appropriate authority to effect the decontrol under the authorizing law, regulation, or Government-wide policy;

2. When the designating agency decides to release the CUI to the public by making an affirmative, proactive disclosure;

3. When an agency discloses it in accordance with an applicable information access statute, such as FOIA, or the Privacy Act (when legally permissible), provided the designator's agency incorporates such disclosures into its public release processes; or

4. When a pre-determined event or date occurs, as described in 32 CFR § 2002.20(g), unless law, regulation, or Government-wide policy requires coordination first.

C. A designating agency may also decontrol CUI:

1. In response to a request from an authorized holder to decontrol it; or

2. Concurrently with any declassification action under Executive Order 13526 or any predecessor or successor order, if the information also appropriately qualifies for decontrol as CUI.

D. An agency may designate in its CUI policies which agency covered individuals/entities it authorizes to decontrol CUI, consistent with law, regulation, and Government-wide policy.

---

[10] In this case, ED would be the "designating agency."

[11] An authorized holder is any person who lawfully possesses CUI. Because almost all ED covered individuals/entities and their affiliated parties will encounter CUI while performing work, they are considered to be authorized holders.

E. Decontrolling CUI relieves the requirement to handle the information under the CUI Program but does not constitute authorization for public release.

F. ED covered individuals/entities must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, releasing to the public, or donating the CUI to a private institution. Otherwise, ED covered individuals/entities do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

1. For relatively small documents, all CUI markings within a decontrolled CUI document shall be removed or struck through. For large documents, ED covered individuals/entities may remove or strike through only those CUI markings on the first or cover page of the decontrolled CUI and markings on the first page of any attachments that contain CUI. They shall also mark or stamp a statement on the first page or cover page that the CUI markings are no longer applicable.

2. If ED covered individuals/entities use decontrolled CUI in a newly created document, they must remove all CUI markings for the decontrolled information.

3. Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and ED (or other agency) policies on the public release of information.

4. ED covered individuals/entities may request that the designating agency decontrol CUI that they believe should be decontrolled. See section XXXVII below, Challenges to Designation of Information as CUI.

5. If an authorized holder publicly releases CUI in accordance with the designating agency's authorized procedures, the release constitutes decontrol of the information. CUI markings shall be cancelled prior to public release as described in subparagraph XVII.F (1) above.

6. Unauthorized disclosure of CUI does not constitute decontrol.

7. ED covered individuals/entities must not decontrol CUI in an attempt to conceal, or to otherwise circumvent accountability for, an identified unauthorized disclosure.

8. When laws, regulations, or Government-wide policies require specific decontrol procedures, ED covered individuals/entities must follow such requirements.

9. Records Management Note: The Archivist of the United States may decontrol records transferred to the National Archives in accordance with

32 CFR § 2002.34, absent a specific agreement to the contrary with the designating agency. The Archivist decontrols records to facilitate public access pursuant to 44 U.S.C. 2108 and NARA's regulations at 36 CFR parts 1235, 1250, and 1256.

XVIII. Marking of CUI [§ 2002.20]

A. Any employee, contractor, or other ED affiliated person may mark information as CUI based upon the categories that are listed in the CUI Registry. CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls.

B. Information may not be marked as CUI:

1. To conceal violations of law, inefficiency, or administrative error;

2. To prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency;

3. To improperly or unlawfully interfere with competition;

4. To prevent or delay the release of information that does not require such protection; or

5. If the CUI is required by statute or Executive Order to be made available to the public or if it has been released to the public under proper authority.

C. The 32 CFR part 2002 and supplemental guidance issued by the NARA CUI EA (e.g., the CUI Marking Handbook) shall be followed for the marking of CUI on paper and electronic documents. Appendix D to this Directive augments the information in the MARKING GUIDE.

1. The CUI banner marking. Designators of CUI must mark all CUI with a CUI banner marking. The content of the CUI banner marking must be inclusive of all CUI within the document and must be the same on each page. Banner markings must appear at the top of each page of any document that contains CUI, including email transmissions. Banner markings may include up to three elements:

a. The CUI control marking. The CUI control marking may consist of either the word "CONTROLLED" or the acronym "CUI," at the designator's discretion. The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of CUI basic categories. If portion markings (see section XIX below) are used, **all**

pages shall display CUI banner markings. Computer screens shall also display a CUI banner on each screen that contains CUI.

1) CUI category marking: These are mandatory to include in the CUI banner marking for categories of CUI that are listed in the CUI Registry as being CUI Specified. If any part of the document contains CUI Specified, then the applicable category marking must appear in the banner, preceded by a "SP-" to indicate the specified nature of the category (e.g., CUI//SP-PCII).

2) Marking and any category markings are separated by a double forward slash (i.e. //). When including multiple categories in the banner, they must be alphabetized, with specified categories appearing before any basic categories. Multiple categories in a banner line must be separated by a single forward slash (i.e. /).

3) Limited Dissemination Control Markings.

   a) NARA has published a list of several Limited Dissemination Control markings that can be applied based on ED's own criteria. These markings will appear in the CUI Registry and will include such controls as FED ONLY (Federal Employees Only), NOCON (No dissemination to contractors), and DL ONLY (Dissemination authorized only to those individuals or entities on an accompanying distribution list). Limited Dissemination Control Markings are preceded by a double forward slash (i.e., //) and appear as the last element of the CUI banner marking.

   b) ED covered individuals/entities may only apply Limited Dissemination Control Markings to CUI to bring attention to any dissemination control called for in the underlying authority or to limit the dissemination of CUI. Limited Dissemination Control Markings should be used only after careful consideration is given to the potential impacts to the timely dissemination of the information to authorized recipients.

2. Other Markings or Statements on the Document.

   a. Marking: Specific marking, disseminating, informing, distribution limitation, or warning statements that are required by underlying authorities may be additionally placed on the document, but not within the banner or portion markings. These markings or indicators must be placed on the document as prescribed by the underlying law, regulation, or Government wide policy. Questions regarding the placement of such markings may be referred to the responsible authority for the information, or to the ED CUI Program Manager or

principal office CUI POC at (CUIProgram@ED.gov) or contact information as disseminated by each ED principal office.

b. Identification of the designator (i.e., CUI designation indicator)

1) Designator: All documents containing CUI must identify the office that designated the CUI (the designator) on the first page or cover. This should include the ED principal office and office within that principal office, e.g., letterhead and/or FROM line; or by adding a "Controlled by" line at the bottom of the first page (for example, "Controlled by: OST, ED"). See Appendix D for an example.

2) CUI decontrolling indicators: Where feasible, a specific decontrolling date or event shall be included with all CUI. This may be accomplished in a manner that makes the decontrolling schedule readily apparent. See Appendix D for an example.

a) When used, decontrolling indicators must use the format: "Decontrol On (YYYYMMDD):" or "Decontrol On (specific event)." See Appendix D for an example.

b) Decontrol is presumed at midnight local time on the date indicated. If CUI is marked with a decontrol date, no further review by, or communication with, the designator is required at the time when CUI is decontrolled.

c) If using a specific event after which the CUI is considered decontrolled:

i. The event must be foreseeable and verifiable – not based on or requiring special access or knowledge (e.g., the day of a press release, or after a dignitary has made a visit, or after a special operation has been completed); and

ii. A point of contact and preferred method of contact shall be included in the decontrol indicator to allow verification that a specified event has occurred.

D. Incorrectly Marked Documents. If ED covered individuals/entities believe that CUI is marked incorrectly, please notify the ED CUI Program Manager or designated principal office CUI POC.

E. Re-Marking of Legacy-Marked Information.[12] Due to the quantity of legacy-marked information within the Department, the burden that would result from re-marking all legacy information makes such an effort impractical. Instead, per 32 CFR § 2002.38(b) the following applies:

1. Legacy Marking: Information containing legacy markings (e.g., FOUO or SBU) need not be re-marked if it remains within ED. ED covered individuals/entities must make users aware of the information's CUI status using an alternate marking method that is clear (for example, through user access agreements, a computer system digital splash screen [e.g., alerts that flash up when accessing the system], or signs in storage areas or on containers).

2. Any time legacy information is used to produce new material, or if the legacy information qualifies as CUI and is sent outside the Department, the legacy markings must be removed or struck through, and the appropriate CUI markings applied. This is a firm requirement and must be completed before the information can be released outside of ED. (See also section XXXII below.)

F. The lack of a CUI marking on information that qualifies as CUI does not exempt the holder from abiding by applicable handling requirements as described in this Directive and its references.

G. When it is impractical to individually mark CUI legacy materials due to quantity or nature of the information, **ED covered individuals/entities must make recipients aware of the information's CUI status using an alternate marking method that is readily apparent** (for example, through user access agreements, a computer system digital splash screen (e.g., alerts that flash up when accessing the system), or signs in storage areas or on containers). ED covered individuals/entities must inform the CUI Program Manager of all such instances and identify solutions that will bring the procedures in line with the CUI Program. (32 CFR § 2002.38(b))

XIX. Portion Marking (Optional Except for When CUI Is Combined in Documents with Classified National Security Information (CNSI)) [§ 2002.20(f)]

A. Portion markings are a means to provide information about the sensitivity of a particular section of text, paragraph, bullet, picture, chart, etc. They consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title.

[12] "For Official Use Only" (FOUO) and "Sensitive But Unclassified" (SBU) are legacy markings that are replaced by the CUI makings. See the Definitions section regarding legacy markings.

B. Portion marking is not required except when CUI is combined in documents that also contain CNSI, but it is permitted and encouraged to facilitate information sharing and proper handling, and to assist FOIA reviewers in identifying the CUI within a large document that may be primarily Uncontrolled Unclassified Information. See Appendix C for the description and use of portion markings.

XX. Commingling CUI Markings with CNSI Markings [§ 2002.20(g)]

A. If CNSI documents also contain CUI, the decontrolling provisions of the CUI Program apply only to the CUI portions. If the CUI portion is not clearly marked, the CNSI control applies. In addition, ED covered individuals/entities must adjust the CUI marking scheme to:

1. Portion mark all CUI to ensure that CUI portions can be distinguished from portions containing classified and uncontrolled unclassified information; and

2. Include the CUI control marking, *CUI Specified* category markings, and any limited dissemination control markings in the overall banner marking.

B. The CUI Registry and the NARA CUI MARKING GUIDE contain specific guidance on marking CUI when commingled with CNSI.

XXI. Commingling Restricted Data (RD) and Formerly Restricted Data (FRD) with CUI [§ 2002.20(h)]

A. Restricted Data (RD) and Formerly Restricted Data (FRD) are categories of CNSI concerning nuclear weapons design and utilization.

B. To the extent possible, avoid commingling RD or FRD with CUI in the same document. When it is not practicable to avoid such commingling, follow the marking requirements of the CUI Program as well as the marking requirements for RD and FRD contained in 10 CFR part 1045, Nuclear Classification and Declassification.

C. Follow the marking requirements of 10 CFR part 1045 when extracting an RD or FRD portion for use in a new document.

D. Follow the requirements of the CUI Program as described in this Directive if extracting a CUI portion for use in a new document.

E. Contact the Defense Security Service (DSS) or ED CISO immediately if there is contact with CNSI, RD or FRD data.

XXII. Transmitting/Transporting CUI [§ 2002.14(d)] and [§ 2002.20(i)]

A. Standard commercially available telephone lines are acceptable for the discussion of CUI, but digital information in email and websites should be protected at no less than the FIPS Publication 199 moderate confidentiality level.

B. CUI may be sent through the United States Postal Service (USPS) or any commercial delivery service that offers in-transit automated tracking and accountability tools. However, beginning in 2022, under the Social Security Number Fraud Prevention Act of 2017, Pub. L. No. 115-59 (2017), full Social Security numbers of individuals may not be sent through the mail, unless the Secretary has issued regulations that specify the circumstance(s) under which their inclusion on a document sent by mail is necessary.

C. CUI may also be sent through interoffice or interagency mail systems.

D. Address packages that contain CUI for delivery **only** to a specific recipient, not to an office or organization. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI.

XXIII. Transmittal Document Marking Requirements [§ 2002.20(j)]

A. When a transmittal document accompanies CUI, the transmittal document must include on its face a distinctive notice that CUI is attached or enclosed. This serves to notify the recipient about the sensitivity of the document beneath the cover letter.

B. The notice shall include the CUI marking ("CONTROLLED" or "CUI") along with the following or similar instructions, as appropriate:

1. "When enclosure is removed, this document is Uncontrolled Unclassified Information"; or

2. "When enclosure is removed, this document is (indicate control level);" or, "upon removal, this document does not contain CUI."

XXIV. Reproduction of CUI [§ 2002.14(e)]

A. CUI may be reproduced (e.g., copy, scan, print, electronically duplicate) in furtherance of a lawful Government purpose; and

B. When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, management officials must ensure that the equipment does not retain data, transmit the data to a non-federal entity, and

they must otherwise sanitize it in accordance with NIST SP 800-53. The multifunction printers at facilities are protected against the inadvertent release of CUI to unauthorized covered individuals/entities by login procedures and meet this requirement. Users in other locations should check with their equipment provider or their information technology office to determine whether the equipment retains information for any amount of time after it is processed, and how to clear the equipment of the information if necessary. This information should be posted on any equipment that retains data.

XXV. Working Papers [§ 2002.20(k)]

A. Working papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

B. Working papers containing CUI must be marked the same way as the finished product containing CUI would be marked and as required for any CUI contained within them. Working papers must be protected as any other CUI. This applies whether or not the working papers will be shortly destroyed. When no longer needed, working papers shall be destroyed in accordance with section XV above.

XXVI. Using Supplemental Administrative Markings with CUI [§ 2002.20(l)]

A. Supplemental administrative markings (*e.g.* "Pre-decisional," "Deliberative," "Draft") may be used with CUI. The NARA CUI MARKING GUIDE provides examples of supplemental administrative markings.

B. Supplemental administrative markings may not impose additional safeguarding requirements or disseminating restrictions or designate the information as CUI. Their purpose is to inform recipients of the status of documents under development to avoid confusion and maintain the integrity of a decision-making process.

C. Supplemental markings other than the universally-accepted "DRAFT," shall, on the first page or the first time it appears, include an explanation or intent of the marking, e.g., Pre-decisional – "The information in this document provides background, options, and/or recommendations about [topic]. It is not yet an accepted policy." (This is an example only…the language may be changed to suit the topic.)

D. Supplemental markings may not appear in the CUI banners, nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings.

E. Supplemental administrative markings must not duplicate any CUI marking described in the CUI Registry.

XXVII. Unmarked CUI [§ 2002.20(m)]

Unmarked information that qualifies as CUI should be marked and treated appropriately as described in this CUI Program. Unmarked legacy information, that qualifies as CUI, because of the exception allowed in section XVIII E. above of this Directive must still be handled (e.g., safeguarded, stored, and destroyed) in accordance with CUI requirements.

XXVIII. CUI Self-Inspection Program [§ 2002.24]

In accordance with 32 CFR § 2002.8(b)(4), ED will implement a Self-Inspection Program as follows:

1. The CUI Program Manager, under the authority of the CUI SAO, shall provide technical guidance, training, and materials to ensure that ED principal offices conduct reviews and assessments of their CUI Programs at least annually, and report the results to the ED CUI Program Manager as required by the NARA CUI EA;

2. Following training of the designated CUI POCs of each ED principal office, ED principal offices shall conduct annual self-inspections of their CUI Program and report the results on a schedule determined by the CUI SAO. ED principal offices shall include in the self-inspection any contractor companies that are under their purview by on-site inspections, or by examining any self-inspections conducted by the contractor company;

3. Following guidance and inspection materials received from the ED CUI Program Manager, self-inspection methods, reviews, and assessments shall serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;

4. The CUI Program Manager shall provide to the ED principal offices formats for documenting self-inspections and recording findings, and provide advice for resolving deficiencies and taking corrective actions; and

5. Results from the Department-wide self-inspections shall be used to inform updates to the CUI training provided to ED covered individuals/entities.

XXIX. Education and Training [§ 2002.30]

A. Every ED employee, contract employee, and affiliated person who may encounter CUI in their work shall complete formal CUI training prior to obtaining access to CUI. Refresher training shall be required every two years

after the initial training. Individual training will be computer-based, classroom, or desk-side, depending upon the circumstances. If applicable, ED covered individuals/entities must also take training for any CUI Specified categories to which they have access or which they are required to safeguard.

B. CUI training must ensure that ED covered individuals/entities who have access to CUI receive training on designating CUI, relevant CUI categories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures. See CUI Notice 2017-01 for specific training elements that must be conveyed in initial and refresher training.

C. Continuing periodic education shall be provided using brochures, posters, ED web or SharePoint pages, or other methods.

XXX. CUI Cover Sheets [§ 2002.32]

A. ED covered individuals/entities may use a cover sheet for CUI, but their use is optional. SF 901 is the correct cover sheet. Standard Form 901 replaces forms OF901, OF902 and OF903, which were rescinded on December 14, 2018. Agencies may continue to use Forms OF901, OF902, and OF903 until existing supplies have been depleted. Cover Sheets may be obtained from the NARA or downloaded from GSA https://www.gsa.gov/cdnstatic/SF901-18a.pdf?forceDownload=1 and then reproduced by user offices

B. ED covered individuals/entities may use cover sheets to identify CUI and to serve as a shield to protect the attached CUI from inadvertent disclosure.

C. Cover sheets may be filed along with the hard copy of the information they are protecting, but consideration should be made regarding the extra space in file cabinets that such a practice would require. It is acceptable to file CUI without the cover sheet attached.

XXXI. Transferring Records to NARA [§ 2002.34]

A. When feasible, records containing CUI shall be decontrolled prior to transferring to NARA.

B. If records cannot be decontrolled before transferring to NARA, the following procedures shall be followed:

1. Indicate on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI (subject to NARA's regulations on transfer, public availability, and access; see 36 CFR parts 1235, 1250, and 1256); and

2. For hard copy transfer, do not place a CUI marking on the outside of the container or envelope. Double-wrapping is not required, but if used, only the interior envelope should be marked as "Controlled" or "CUI."

C. If status as CUI is not indicated on the TR or SF 258, NARA may assume the information was decontrolled prior to transfer, regardless of any CUI markings on the actual records. Therefore, ED covered individuals/entities shall clearly indicate the CUI status (whether it is still active or decontrolled) prior to transfer.

XXXII. Legacy Materials [§ 2002.36]

A. If any information from legacy documents that qualifies as CUI is re-used, whether the documents have obsolete control markings or not, the newly-created documents (or other re-used ones) must be designated as CUI and marked accordingly.

B. Follow the instructions regarding the marking of legacy materials in section XVIII E. above.

XXXIII. Waivers of CUI Requirements [§ 2002.38]

A. In exigent circumstances,[13] the Secretary or ED CUI SAO may waive certain requirements of the CUI Program for any CUI while it is within ED's possession or control, unless specifically prohibited by applicable laws, regulations, or Government-wide policies.

B. Exigent circumstances waivers may apply when ED shares the information with other agencies or non-Federal entities. In such cases, recipients must be made aware of the CUI status of any disseminated information.

C. If ED designates information as CUI but determines that marking it as CUI is excessively burdensome, the ED CUI SAO also may approve waivers of all or some of the CUI marking requirements while that CUI remains within the Department's control. As noted in section XVIII E. above, the ED CUI SAO has approved a waiver of the removal of ED's legacy markings and re-marking such information as CUI, but only while such information remains under the Department's control.

D. Per 32 CFR § 2002.38(d), the following conditions apply to all waivers. CUI marking waivers, approved by the ED CUI SAO, apply to CUI subject to the waiver only while ED continues to possess that CUI. No marking waiver may accompany CUI when an authorized holder disseminates it outside of ED.

[13] Exigent circumstances exist when following proper procedures would cause an unacceptable delay due to the urgency of the situation.

CUI markings must be uniformly and conspicuously applied to all CUI prior to disseminating it outside ED unless otherwise specifically permitted by the NARA CUI EA. When the circumstances requiring the waiver end, the waiver will be terminated and all requirements for CUI subject to the waiver must be reinstituted without delay. The CUI SAO must detail in each waiver the alternate protection methods the Department will employ to ensure protection of CUI subject to the waiver.

E. Per 32 CFR § 2002.38(e), the CUI SAO shall:

1. Retain a record of each waiver;

2. Include a description of all current waivers and waivers issued during the preceding year in the annual report to the NARA CUI EA, along with the rationale for each waiver and the alternate steps the Department takes to ensure sufficient protection of CUI; and

3. Notify authorized recipients and the public of these waivers through means such as notices or websites.

XXXIV. CUI and Disclosure Statutes [§ 2002.44]

A. General policy. The fact that information is designated as CUI does not prohibit its disclosure if the disclosure is made according to criteria set out in a governing law.

B. CUI and the FOIA. FOIA may not be cited as a CUI safeguarding or disseminating control authority for CUI. When determining whether to disclose information in response to a FOIA request, the decision must be based upon the content of the information and applicability of any FOIA statutory exemptions, regardless of whether or not the information is designated or marked as CUI. There may be circumstances in which CUI may be disclosed to an individual or entity, including through a FOIA response, but such disclosure does not always constitute public release as defined by the CUI Program. Although disclosed via a FOIA response, the Department may still need to control CUI while ED continues to hold the information, despite the disclosure, unless ED otherwise decontrols it (or ED includes in its policies that the FOIA disclosure always results in public release and the CUI does not otherwise have another legal requirement for its continued control).

C. CUI and the Whistleblower Protection Act. The CUI Program does not change or affect existing legal protections for whistleblowers. The fact that information is designated or marked as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority

and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation Executive Order or directive.

XXXV. CUI and the Privacy Act [§ 2002.46]

The fact that records, or individually identifiable information in records, are subject to the Privacy Act does not mean that the Privacy Act is the sole reason for marking the records or individually identifiable information therein, as CUI. Individually identifiable information contained in records that are maintained in a Privacy Act system of records may also be subject to controls under other CUI categories and may need to be marked as CUI for that reason. In addition, when determining whether certain individually identifiable information must be protected under the Privacy Act or whether the Privacy Act allows the release of such individually identifiable information to an individual or entity, the Department's decision to protect or release the information must be based on both the content of the information and the Privacy Act's requirements, regardless of whether the information is designated or marked as CUI.

XXXVI. CUI and the Administrative Procedure Act (APA). [§ 2002.48]

Nothing in the CUI Program regulations alters the Administrative Procedure Act (APA) or the powers of Federal administrative law judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor does the CUI Program impose requirements concerning the manner in which ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

XXXVII. Challenges to Designation of Information as CUI [§ 2002.50]

A. Authorized holders of CUI who, in good faith, believe that a designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the ED CUI Program Manager. Challenges may be made anonymously; and challengers cannot be subject to retribution for bringing such challenges.

B. If the information at issue is involved in Government litigation, or the challenge to its designation or marking as CUI arises as part of the litigation, the issue of whether the challenger may access the information will be addressed via the litigation process instead of by the ED CUI Program Manager. Challengers should nonetheless notify the ED CUI Program Manager of the issue through the Department's process described below and include its litigation connection.

C. If any ED principal office receives a challenge, the CUI POC for that office shall work with the ED CUI Program Manager to take the following measures:

1. Acknowledge receipt of the challenge;
2. Provide an expected timetable for response to the challenger;
3. Review the merits of the challenge with a SME;
4. Offer an opportunity to the challenger to define a rationale for belief that the CUI in question is inappropriately designated;
5. Notify the challenger of the Department's decision; and
6. Provide contact information of the official making the decision in this matter

D. Until the challenge is resolved, the challenged CUI should continue to be safeguarded and disseminated at the control level indicated in the markings.

E. If a challenging party disagrees with the Department's response to a challenge, that party may use the Dispute Resolution procedures described in 32 CFR § 2002.52.

XXXVIII. Misuse of CUI and Incident Reporting [§ 2002.54]

A. Suspected or confirmed CUI misuse shall be reported to the Education Security Operations Center (EDSOC) within 1 hour upon discovery of potential misuse of CUI. The EDSOC will process the incident per the EDSOC procedures. All relevant covered individuals/entities will be notified appropriately. Consistent with Departmental Directive, "Cooperation With and Reporting to the Office of Inspector General," (OIG: 1-102), reports and referrals to the OIG should be made if appropriate.

B. After EDSOC has completed its investigation, resultant sanctions shall be applied in accordance with applicable human capital policies. Misuse of CUI that has been designated by another Executive department or agency shall be reported to that agency by the CUI POC of the offending principal office.

XXXIX. Sanctions for Misuse of CUI [§ 2002.56]

Employee misuse of CUI may be considered misconduct and may therefore be subject to the procedures set forth in HCP 751-1, Discipline and Adverse Actions, or, for employees who are serving a probationary or trial period, to the procedures set forth in HCP 315-1, Probationary Periods, or to any successor procedures. Any sanctions specifically established by laws, regulations, or

Government-wide policies governing certain categories of CUI may be applied. to preserve the independence of the OIG, any suspected misuse of CUI by OIG employees should also be reported to the OIG for appropriate handling, including the determination of sanctions.

XL. Publication of CUI

A. Publication of CUI or its posting on public websites or social media is prohibited unless the CUI has been properly decontrolled in accordance with section XVII above.

B. ED CUI Program Manager and designated CUI POC's will routinely check publically facing websites to ensure that CUI is not posted or present.

XLI. Requesting New or Modification to CUI Categories

A. ED covered individuals/entities who encounter information described in law, regulations, or Government-wide policy that is not described in the CUI Registry may recommend that a new CUI category be entered into the CUI Registry or that existing CUI categories be revised in the CUI Registry.

B. ED covered individuals/entities should submit their recommendation through their CUI Point of Contact. The CUI POC shall coordinate through the ED CUI Program Manager. The request should include:

1. A description of the CUI to be marked or to be revised and the reasons for any suggested marking or revision;

2. The law(s), regulation(s), or Government-wide policy (-icies) that apply; and

3. A suggested name, along with a suggested acronym for the category.

C. The ED CUI Program Manager, in coordination with the ED General Counsel or designee, will submit the recommendation to the NARA CUI EA.

APPENDIX A: Acronyms

CISO – Chief Information Security Officer

CFR – Code of Federal Regulations

CNSI – Classified National Security Information

CUI – Controlled Unclassified Information

CUI PMO – Controlled Unclassified Information Program Management Office

DSS – Defense Security Service

EA – Executive Agent

EDAR – Department of Education Acquisition Regulation

EDSOC - Education Security Operations Center

FAR – Federal Acquisition Regulation

FIPS – Federal Information Processing Standards

FOIA – Freedom of Information Act

FRD – Formerly Restricted Data

FSA – Federal Student Aid

ISOO – Information Security Oversight Office

ISSO – Information Systems Security Officer

NARA – National Archives and Records Administration

OCIO – Office of the Chief Information Officer

OIG – Office of Inspector General

OMB – Office of Management and Budget within the Executive Office of the President

PMO – Program Management Office

RD – Restricted Data

SAO – The designated Senior Agency Official [for CUI]

SBU – Sensitive But Unclassified

TR – Transfer Request in NARA's Electronic Records Archives (ERA)

APPENDIX B: Definitions

The following terms are associated with the CUI Program. Additional definitions may be found in 32 CFR § 2002.4.

A. **Affiliated parties** – Consultants, researchers, organizations, and State, local, Tribal, and private sector partners with whom ED shares CUI. Individuals who have no contact with ED CUI are excluded from this definition.

B. **Authorized holder** – Any person who lawfully possesses CUI. Because almost all ED covered individuals/entities and their affiliated parties will encounter CUI while performing work, they are considered to be authorized holders. (See also Lawful Government Purpose.)

C. **Banner** – A distinctive marking across the top and/or bottom of a document (paper or electronic) that provides information or a caution about the contents of the document.

D. **Controlled Environment** – Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

E. **Controlled Unclassified Information (CUI)** – Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an executive branch agency to handle using safeguarding or dissemination controls.

F. **CUI Basic** – The subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Executive branch agencies handle *CUI Basic* according to the CUI Program's uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry. *CUI Basic* differs from *CUI Specified* (see definition for *CUI Specified* in this section), and *CUI Basic* controls apply whenever *CUI Specified* ones do not cover the involved CUI.

G. **CUI Categories** – Those types of information for which laws, regulations, or Government-wide policies require or permit executive branch agencies to exercise safeguarding or dissemination controls, and which the NARA CUI EA has approved and listed in the CUI Registry.

H. **CUI Category Markings** – The markings approved by the NARA CUI EA for the CUI categories are listed in the CUI Registry.

I. **CUI Executive Agent** – The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and

oversees executive branch agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

J. **CUI Program** – The executive branch agency-wide program to standardize CUI handling by all executive branch agencies. The Program includes the rules, organization, and procedures for CUI, established the Order, 32 CFR part 2002, and the CUI Registry. This Directive implements the CUI Program within ED.

K. **ED CUI Program Manager** – The ED official, designated by the ED CUI SAO, to serve as the official representative to the NARA CUI EA on ED's day-to-day CUI Program operations, both within ED and in interagency contexts.

L. **CUI Program Management Office** – The CUI PMO is responsible for implementing the CUI Program as described above. This office is located in the Office of the Chief Information Officer (OCIO), Information Technology Program Services (ITPS) branch.

M. **CUI Point of Contact (CUI POC)** – A principal office's appointed employee who is assigned specific duties to assist the ED CUI Program Manager in implementing and managing the CUI Program.

N. **CUI Registry** – The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the NARA CUI EA. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures for unclassified information that requires safeguarding or dissemination controls. The CUI Registry may be easily located by entering "CUI Registry" in any web browser. The full URL is http://www.archives.gov/cui/registry/category-list.html.

O. **CUI Specified** – The subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information.

P. **Decontrol** – The removal of safeguarding or dissemination controls from CUI that no longer requires such controls.

Q. **Defense Security Services** – The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) that provides the military services, Defense

Agencies, 31 federal agencies and approximately 13,500 cleared contractor facilities with security support services.

R. **Designating Agency** – Any executive branch agency that designates or approves the designation of a specific item of information as CUI. 32 CFR § 2002.4(u).

S. **Designators of CUI** – Employees, contractors, or other ED affiliated persons who mark information as CUI based upon the CUI categories that are listed in the CUI Registry. "Designator" may also refer to the organization that designates information as CUI.

T. **Disseminating Agency or Organization** – Any organization that distributes CUI by transmitting it to an authorized holder or by placing onto accessible media such as SharePoint, a website, or electronic bulletin board.

U. **ED Principal Office** – For the purpose of this Directive, a Principal Office is an organization headed by an Assistant Secretary or equivalent.

V. **ED covered individuals/entities** – For the purposes of this Directive, ED covered individuals/entities include ED employees, contractors (on-site and off-site) who agree to comply with the terms and conditions of this Directive, and affiliated parties such as consultants, researchers, organizations, and State, local, Tribal, and private sector partners with whom ED may share CUI who agree to comply with the terms and conditions of this Directive.

W. **Executive Branch Agency -** Executive branch agency, as defined in 5 U.S.C. 105; refers to the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

X. **Federal Information System** – An information system used or operated by ED or by an ED contractor or other organization on behalf of ED. An information system operated on behalf of ED provides information processing services to the Department that the Government might otherwise perform itself but has decided to outsource. This includes systems operated exclusively for Government use and systems operated for multiple users (multiple Federal agencies or Government and private sector users).

Y. **Formerly Restricted Data** – See Restricted Data.

Z. **Lawful Government Purpose** – Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as State and local law enforcement).

AA. **Legacy Markings** – Markings that were in use before the advent of the CUI Program, e.g., For Official Use Only (FOUO) and Sensitive But Unclassified (SBU). Some legacy markings are carried over to the CUI Program (e.g., Sensitive Security Information (SSI), and some are discontinued (e.g., FOUO and SBU).

BB. **Limited Dissemination Controls –** Any CUI EA-approved control that agencies may use to limit or specify CUI dissemination. Limited dissemination of information is necessary to protect intelligence sources, methods, and activities. Limited dissemination manages the distribution of information to a select group of individuals.

CC. **Non-Federal Information System** – Any information system that does not meet the criteria for a Federal information system. When a non-executive branch entity receives Federal information only incidental to providing a service or product to the Government other than processing services, its information systems are not considered Federal information systems. NIST SP 800-171 defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of the CUI Program.

DD. **Protected Communications** – Means of transmission of information that is reasonably expected to be available only to authorized covered individuals/entities.

EE. **Restricted Data (RD) and Formerly Restricted Data (FRD)** – Categories of classified information (classified under the Atomic Energy Act defined in 10 CFR part 1045, Nuclear Classification and Declassification) concerning nuclear weapons design and utilization. Despite the misleading nature of the phrase "Formerly Restricted Data," documents with this marking remain sensitive and must be protected.

FF. **Senior Agency Official (SAO)** – The senior ED official responsible for oversight of ED's CUI Program implementation, compliance, and management.

GG. **Uncontrolled unclassified information** – Information that neither the Order nor classified information authorities cover as protected. Although this information is not controlled or classified, executive branch agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.

HH. **Underlying Authority** – The law, regulation, or Government-wide policy that is the basis for designating information as CUI.

II. **Working papers** – Documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

APPENDIX C: Marking

CUI Banner Marking

- The primary marking for all CUI is the CUI Banner Marking. This is the main marking that appears at the top of any document that contains CUI.
- This marking is MANDATORY for all documents containing CUI.
    - The marking of the CUI Banner must include all elements applicable to the document.
    - The Banner Marking should appear as ***bold CAPITALIZED black text and be centered.***
    - If there is commingling (both CUI and uncontrolled information in the same document), use portion marking to identify each paragraph by marking them either (CUI) or (U). Then if the CUI paragraphs are removed the document can be uncontrolled.
    - The same banner marking must be used on each page even if portion marking is used and not all pages contain CUI.
    - As a best practice, keep the CUI and uncontrolled information in separate portions to the greatest extent possible to allow for maximum information sharing.
- The CUI Banner Markings shall be as follows:
    - The word CONTROLLED will be used as the banner marking on every page of any CUI document. (Information received from an outside agency with CUI as the banner marking should be treated the same as CONTROLLED.)
    - CUI Specific and CUI Basic. For CUI Basic, categories or other markings are not required, but for CUI Specified they are required. Further discussion on Basic and Specified, and examples of banners are discussed later in this Directive.
    - Limited Dissemination Control Markings. These are preceded by a double forward slash (//) to separate them from the rest of the CUI Banner Marking. **Only Limited Dissemination Control Markings found in the CUI Registry are authorized for use with CUI. See Appendix B.** ED's practice will be to always use dissemination control markings within the Banner Marking.
    - Required Indicators per Authorities. Required indicators-including information, warning, or dissemination statements may be mandated by the law, Federal regulations, or Government-wide policy that makes a specific item of information CUI. These indicators shall not be included in the CUI Banner or portion

markings but must appear in a manner readily apparent to authorized covered individuals/entities and consistent with the requirements of the governing document.

- Supplemental Administrative Markings. Supplemental administrative markings may be used along with CUI to inform recipients of the non-final status of documents. Supplemental administrative markings may not be used to control CUI and may not be commingled with or incorporated into the CUI Banner marking or portion markings. Supplemental administrative markings may not duplicate any marking in the CUI Registry. Administrative markings that can be used for ED CUI documents are Draft, Deliberative, Pre-decisional, or Provisional and should be shown as a watermark behind the text.

CUI Categories

Understanding CUI Categories:

CUI Categories are essentially the different "flavors" of CUI. Each Category is based in a least one (and sometimes many) of the laws, regulations, or Government-wide policies (also referred to as Authorities) that require a certain type of information be protected or restricted in dissemination.

There are two types of CUI Categories: CUI Basic and CUI Specified.

CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry. All rules of CUI apply to CUI Basic Categories, making the handling and marking of CUI Basic the simplest.

CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance. CUI Specified is different, since the requirements for how users must treat each type of information vary with each category. This is because some Authorities have VERY specific requirements for how to handle the type of information they pertain to-requirements that simply would not make sense for the rest of CUI.

CUI Specified is NOT a "higher level" of CUI, it is simply different. And because the things that make it different are dictated in a law, federal regulation, or Government-

wide policy, they are not things that can legally be ignored or overlooked. A document containing multiple CUI Specified Categories must include ALL of them in the CUI Banner Marking.

There is one additional issue with CUI Specified, in that some CUI categories are only CUI Specified ***sometimes.*** As stated above, this is because there are often many different laws or regulations that pertain to the same type of information type, but only ***some*** of them may include additional or alternate handling requirements from CUI Basic. Therefore, only CUI created under those Authorities would be CUI Specified.

Within the CUI Registry (https://www.archives.gov/cui/registry/category-list) click on the appropriate Category and refer to each authorization to determine whether Basic or Specified.

Designation Indicator

All documents containing CUI MUST indicate that ED is the designating agency.

Refer to any one of the examples in Appendix D on ED's requirement and placement of the Designation Indicator.

Every effort should be made to identify a point of contact, branch, or division within an organization, and to include contact information.

Portion Marking

Portion marking of CUI is optional in a fully unclassified document, but is permitted and encouraged to facilitate information sharing and proper handling of the information.

When CUI portion marking is used, these rules must be followed:

A. ED's practice will be to always use dissemination control markings within the portion marking and Banner Marking.

B. CUI portion markings are placed at the beginning of the portion to which they apply and must be used throughout the entire document.

C. CUI portion markings are contained within parentheses and may include up to three elements:

    1. The CUI Control Marking: This is mandatory when portion marking and the acronym "CUI" must be used (the word "Controlled" will not be used in the portion markings).

        a. When used, CUI Category markings are separated from the CUI Control marking by a double forward slash (//).

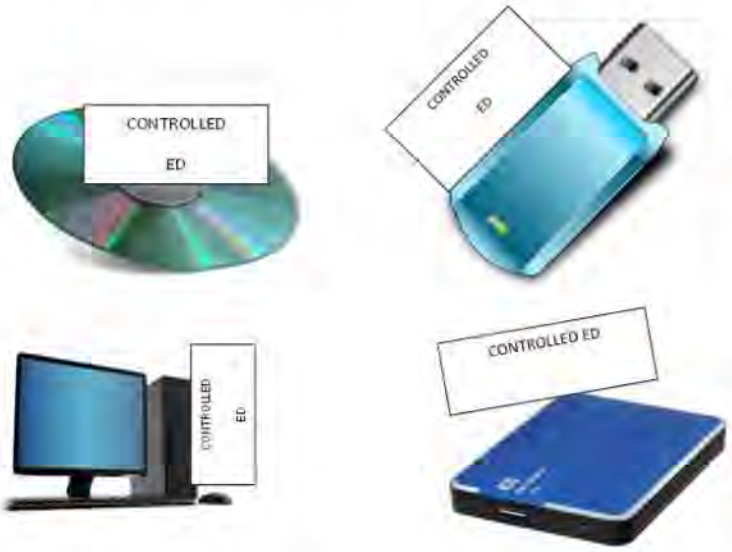
b. When including multiple categories in a portion, CUI Category markings are separated from each other by a single forward slash (/).

2. Limited Dissemination control Markings: These can be found in Appendix B and are separated from preceding CUI markings by a double forward slash (//). When including multiple Limited Dissemination Control Markings, they must be alphabetized and separated from each other by a single forward slash (/).

D. When CUI portion markings are used and a portion does not contain CUI, a "U" is placed in parentheses to indicate that the portion contains uncontrolled information.

Marking Electronic Media Storing or Processing CUI

Media such as USB sticks, hard drives, and CDs must be marked to alert holders to the presence of CUI stored on the device.



Marking Forms with CUI

Forms that contain CUI must be marked accordingly when filled in. If space on the form is limited, cover sheets can be used for this purpose. As forms are updated during agency implementation of the CUI Program, they should be modified to include a statement that indicates the form is CUI when filled in.

CUI Control Marking

CONTROLLED
when filled in

Standard Form 86
Revised December 2010
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U. S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service. ☐ YES ☐ NO

Section 1 - Full Name

Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix.

Last name	First name	Middle name	Suffix
BAUER	JACK	ALLEN	Sr

Section 2 - Date of Birth

Provide your date of birth. *(Month/Day/Year)*
06/25/1969

Section 3 - Place of Birth

Provide your place of birth.

City	County	State	Country *(Required)*
ANYWHERE	THIS COUNTY	AK	United States

Section 4 - Social Security Number

Provide your U.S. Social Security Number.
123-45-6789 ☐ Not applicable

Section 5 - Other Names Used

Have you used any other names? ☐ YES ☒ NO *(If NO, proceed to Section 6)*

Complete the following if you have responded "Yes" to having used other names.

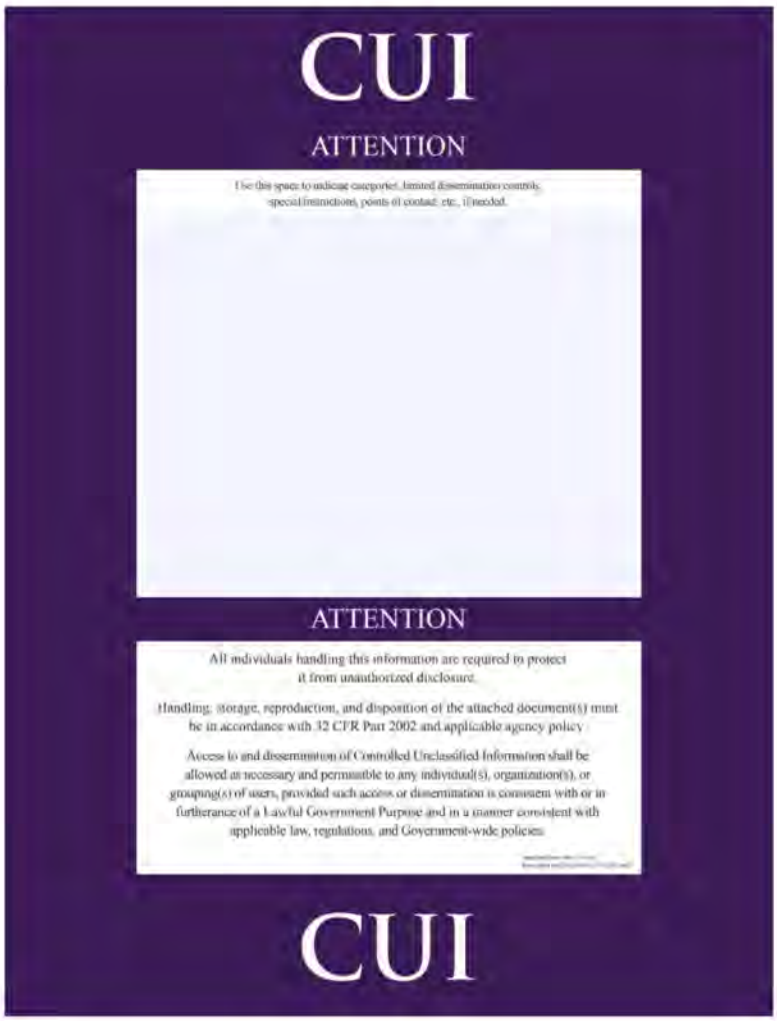
Provide your other name(s) used and the period of time you used it/them [for example: your maiden name(s), name(s) by a former marriage, former name(s), alias(es), or nickname(es)]. If you have only initials in your name(s), provide them and indicate "Initial only." If you do not have a middle name (s), indicate "No Middle Name" (NMN). If you are a "Jr.," "Sr.," etc. enter this under Suffix.

#1 Last name	First name	Middle name	Suffix

From *(Month/Year)* — To *(Month/Year)* ☐ Present — Maiden name? ☐ YES ☐ NO — Provide the reason(s) why the name changed

CUI Cover sheet

The use of a CUI cover sheet is strongly recommended to protect the information and notify people that sensitive information is within. The Standard Form (SF) 901 cover sheet is available for download from the CUI Registry. The SF 901 is shown below.

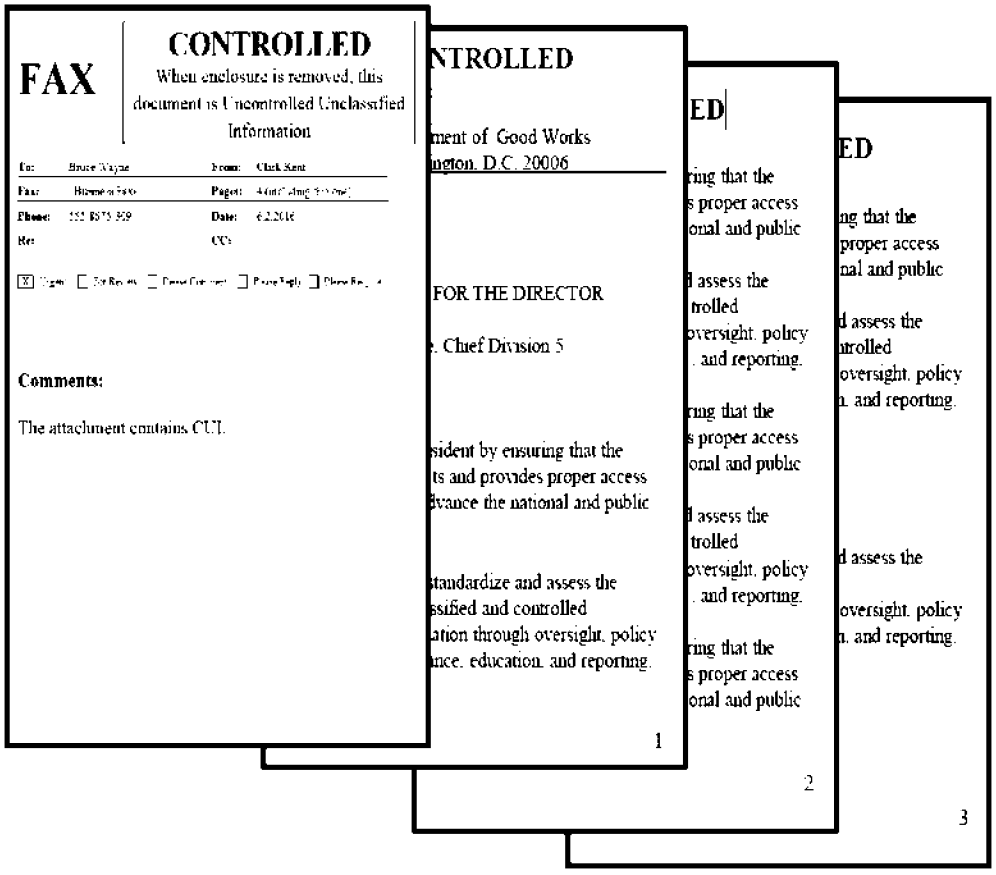


Marking Transmittal Documents

Transmittal document marking requirements:

- When a transmittal document accompanies CUI, the transmittal document must indicate that CUI is attached or enclosed.
- The transmittal document must also include, conspicuously on its face, the following or similar instructions, as appropriate:

- "When enclosure is removed, the document is Uncontrolled", or
- "When the enclosure is removed, this document is (CUI Control Level); upon removal, this document does not contain CUI."

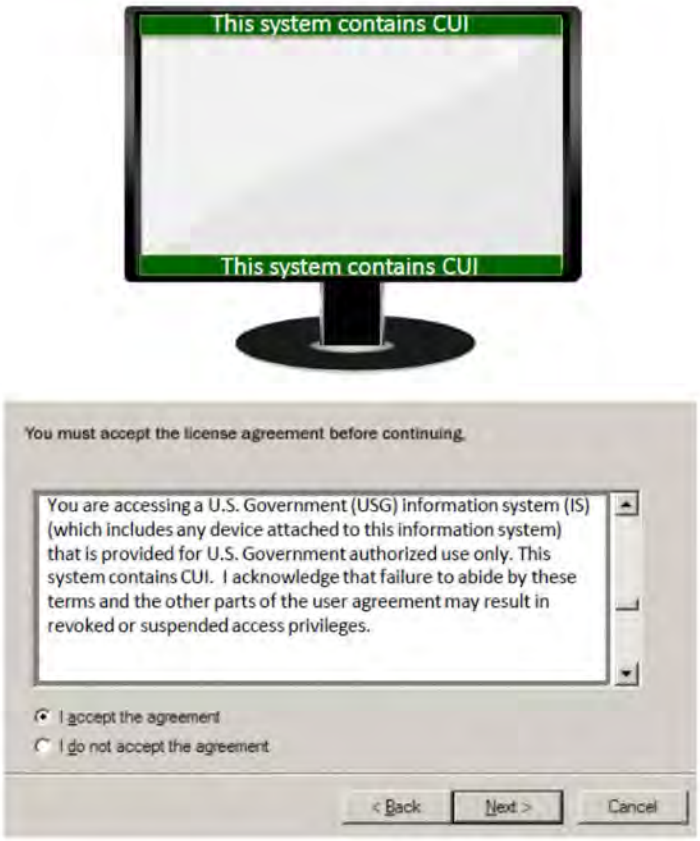


Alternate Marking Methods

Agency heads may authorize the use of alternate marking methods on IT systems, websites, browsers, or databases through agency CUI policy.

These may be used to alert users to the presence of CUI where the agency head has issued a limited CUI marking waiver for CUI designated within the agency.

These warnings may take multiple forms, include these examples:



Room or Area Markings

In areas containing CUI, it may be necessary to alert covered individuals/entities who are not authorized to access it by posting a sign similar to:

Container Markings

When storing CUI, authorized containers must be marked to indicate that it contains CUI.

Shipping and Mailing

When shipping CUI:

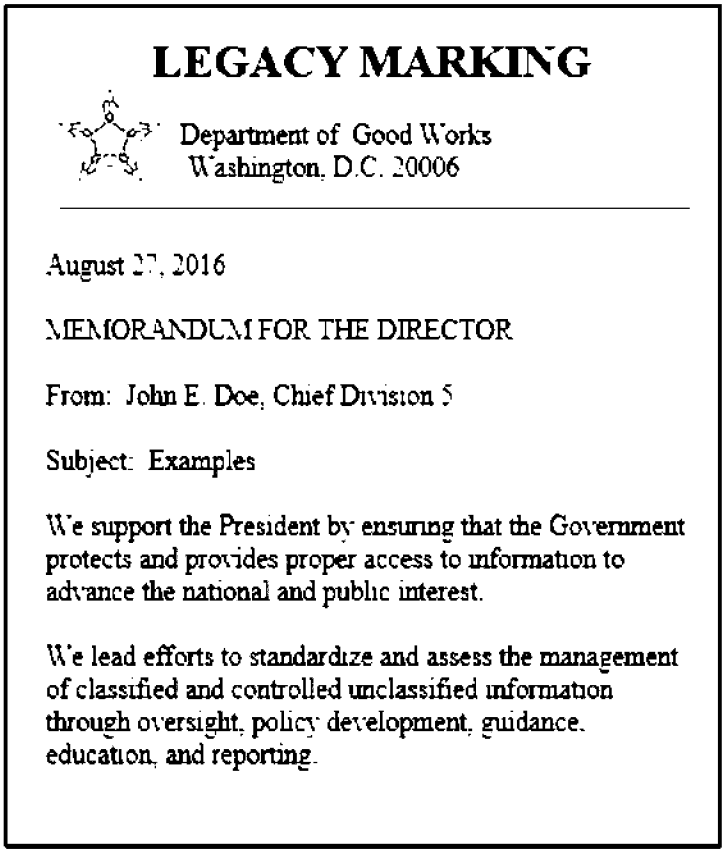
- Address packages that contain CUI for delivery only to a specific recipient.
- DO NOT put CUI markings on the outside of an envelope or package for mailing/shipping.
- Always use in-transit automated tracking and accountability tools to know where a package is at any time.

Re-Marking Legacy Information

Legacy information is unclassified information that was marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program (e.g. PII, SBU, etc.).

All legacy information is not automatically CUI. ED must examine and determine what legacy information qualifies as CUI and mark accordingly.

In cases of excessive burden, the SAO may issue a "Legacy Marking Waiver," as described in 32 CFR § 2002.38(b) of the CUI Rule. As set forth in section XVIII E. of this Directive, the SAO granted a waiver for information containing legacy markings (e.g., FOUO or SBU) if it remains within ED. It need not be remarked as CUI until and unless it is to be "re-used" in a new document.



LEGACY MARKING

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

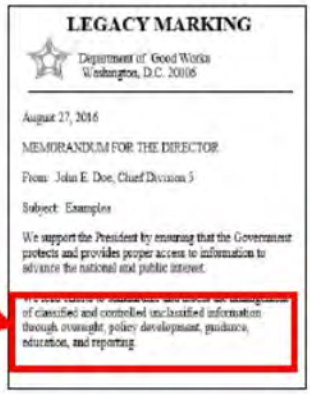
Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Below is the process for evaluating legacy material for remarking. When legacy information is to be re-used and incorporated into another document of any kind (including for external distribution), it must undergo the process described below. *Note: When possible contact the Designator/principal office of the information for guidance in remarking and protecting the legacy information in the CUI Program.*

1. Identify the information that needs to be reused.


LEGACY MARKING

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

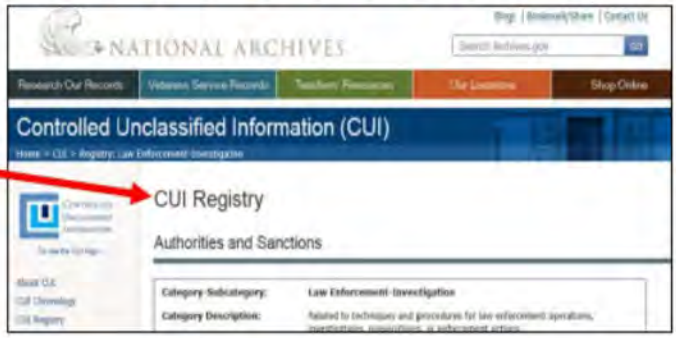
From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting

2. Is the information type listed in the CUI Registry?


NATIONAL ARCHIVES

Research Our Records | Veterans Service Records | Teachers' Resources | Our Locations | Shop Online

Controlled Unclassified Information (CUI)

Home > CUI > Registry: Law Enforcement Investigative

CUI Registry

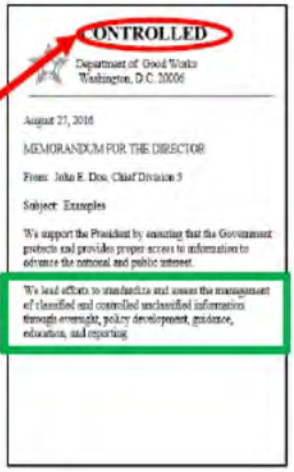
Authorities and Sanctions

Category-Subcategory: Law Enforcement Investigative

Category Description: Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions

3. If the Legacy information type IS listed in the CUI Registry…

…you must mark the new document as CUI.


CONTROLLED

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

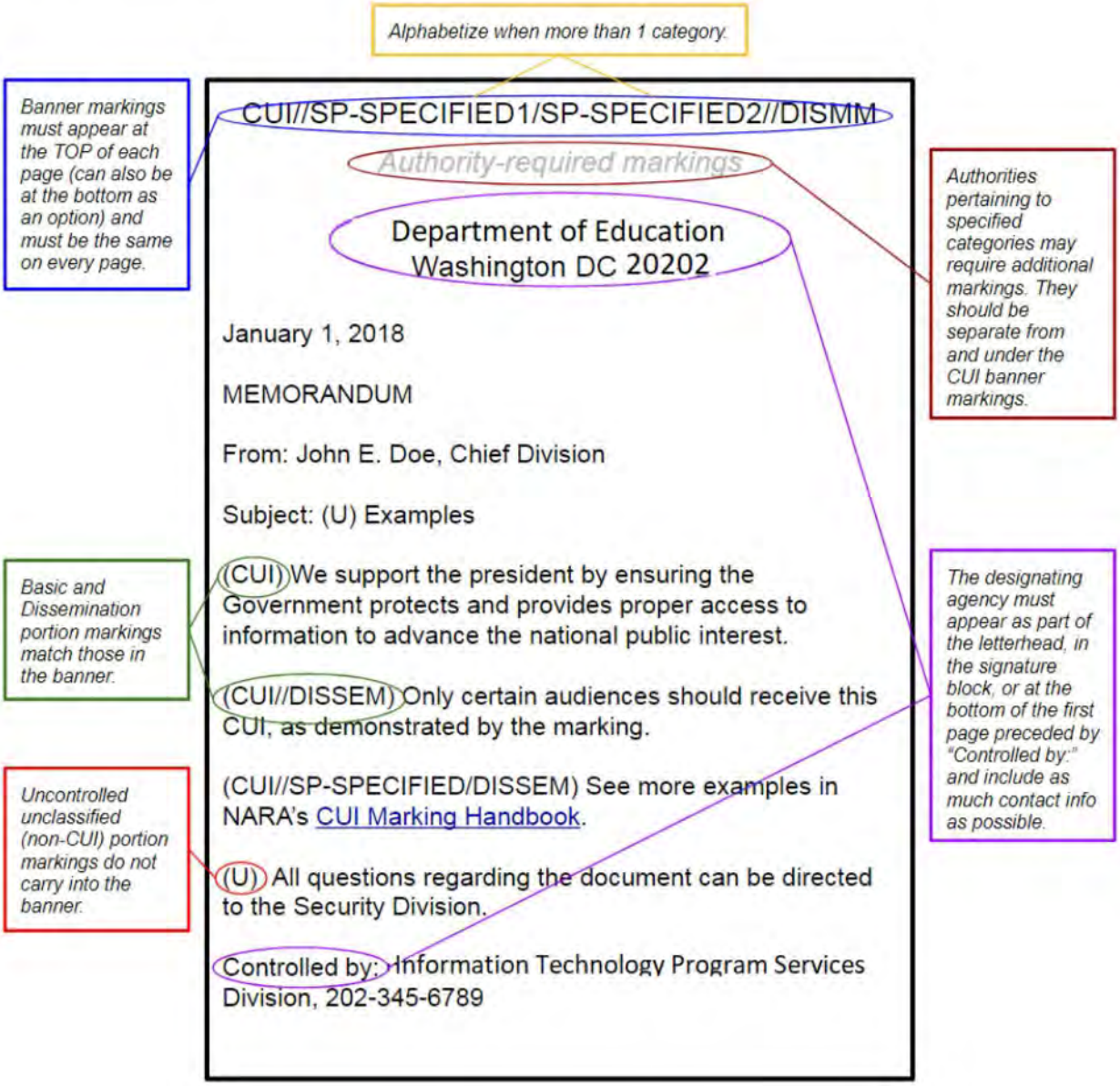
Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting

APPENDIX D: Examples

Example 1: Marking a CUI *Specified* Document



NOTE: The above example uses "SP-SPECIFIED" as a substitute for CUI Category Marking and "DISSEM" as a substitute for Limited Dissemination Control Markings. Appendix B defines the term "Limited Dissemination Controls." To gather actual markings for CUI Categories, go to the following link at: https://www.archives.gov/cui. On the left-hand side of the page choose Category Markings. Click on the desired

Category Name. Here are the explanations of Basic or Specified as well as Safeguarding and or Dissemination Authority.

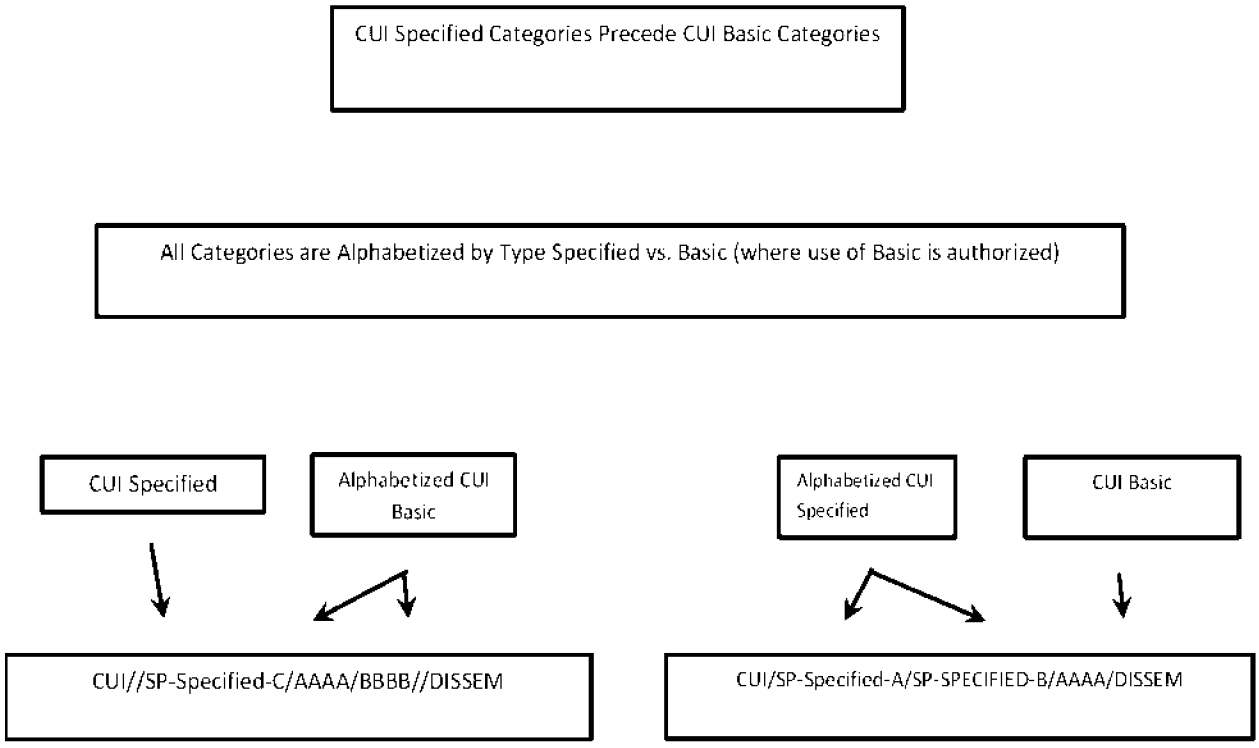
APPENDIX E: Multiple Category Banner Markings: Basic & Specified

CUI Specified Markings MUST precede CUI Basic Category Markings.

CUI Category markings MUST be alphabetized within CUI type (Basic or Specified).

Alphabetized Specified CUI category MUST precede alphabetized Basic CUI categories.

Below are examples of CUI Banner Markings used in a document that contains both CUI specified and CUI Basic.



NOTE: The above examples use "AAAA" and "BBBB" as substitutes for CUI Basic Category, "SP-SPECIFIED-X" as a substitute for a CUI Specified Category Markings, and "DISSEM" as a substitute for a Limited Dissemination Control Marking. Appendix B defines the term "CUI Registry: Limited Dissemination Controls." To gather actual markings for CUI Categories, click on the following link: https://www.archives.gov/cui/registry/category-list. On the left-hand side of the page choose Categories Markings. Within the material you can choose the Category- that fits

your needs; click on the name. Here are the explanations of Basic or Specified as well as Safeguarding and/or Dissemination Authority.