

# Changing Landscape of Data Governance in Higher Education

NEW CYBERSECURITY REGULATIONS

NOVEMBER 6, 2024

BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.



# With You Today



**DAVID CLARK**

Managing Director,  
National Higher Education  
Advisory Services Leader

919-278-1954  
[dclark@bdo.com](mailto:dclark@bdo.com)



**CHRISTINA REYNOLDS**

Assurance Managing Director,  
Industry Specialty Services

703-336-1542  
[creynolds@bdo.com](mailto:creynolds@bdo.com)

# Agenda



Setting the Stage



Exploring a Selection of Existing Data Privacy Rules



Challenges in the Current Landscape



Expected CUI Rule from Department of Education:  
Scoping, Safeguarding, & Self Inspection



Questions

# Setting the Stage



# Setting the Stage



**Privacy**

**vs.**

**Security**



# Existing Data Privacy Rules





# Landscape of Privacy and Security Rules

## EMPLOYEES

- ▶ FCRA
- ▶ ADA

## STUDENTS

- ▶ FERPA
- ▶ FACTA
- ▶ GLBA
- ▶ COPPA
- ▶ Student Aid Internet Gateway Enrollment Agreement

## HEALTH

- ▶ HIPAA
- ▶ HITECH Act

## RESEARCH

- ▶ FISMA
- ▶ “Common Rule”
- ▶ NSPM-33

International Privacy Laws (incl. GDPR)

State Privacy Laws

Electronic Communications Privacy Act

Export Controls

# Family Education Rights and Privacy Act of 1974 (FERPA)

## **PURPOSE & APPLICABILITY:**

Protects the privacy of student education records. Applicable to all educational institutions receiving funding from the U.S. Department of Education.

## **Rights:**

- ▶ Students can access their records and request amendments if believe to be inaccurate or misleading
- ▶ Consent is required to release information

## **Compliance:**

- ▶ Institutions must have written permission to release any information from a student's education record
- ▶ Must provide annual notification of rights



# What constitutes a student record?

## STUDENT RECORD

- ✓ Grades and Transcripts
- ✓ Class Schedule(s)
- ✓ Disciplinary Records
- ✓ Financial Information
- ✓ Contact Information\*
- ✓ Health Records\*

## EXCLUDED

- ✗ Personal/Individual Notes
- ✗ Law Enforcement Records
- ✗ Medical Records
- ✗ Employment Records\*

\*Source: <https://www.archives.gov/cui/registry/category-detail/student-records>

# Health Insurance Portability and Accountability Act (HIPAA)

## **PURPOSE & APPLICABILITY:**

Protects the use and disclosure of protected health information (PHI). Applies to health plans, healthcare providers, healthcare clearinghouses (e.g., billing agencies) and business associates.

HIPAA contains both a Privacy Rule (governing the use of information) and a Security Rule (governing the protection of information)

## **Rights:**

- ▶ May not use or disclose PHI unrelated to treatment, payment, and healthcare operations or other circumstances allowed by the Privacy Rule
- ▶ May disclose if authorized or directly requested by the individual
- ▶ Must disclose to DHHS when undertaking a compliance investigation or review)

## **Compliance:**

- ▶ Application of “reasonable safeguards” to protect and prevent disclosure
- ▶ Documented policy
- ▶ Security Rule: maintain “reasonable and appropriate” administrative, technical, and physical safeguards for protecting e-PHI

# What constitutes PHI?

## PHI

- ▶ Patient identifiers (name, address, SSN, date of birth, etc.)
- ▶ Past, present or future physical or mental health condition
- ▶ Details of healthcare provided to an individual
- ▶ Past, present or future payment details for healthcare services

## EXCLUDED

- ▶ Appointment inquiries
- ▶ Employment or education records subject to FERPA
- ▶ Data collected by wearable devices and health/fitness apps

# National Security Presidential Memorandum (NSPM) 33

## **PURPOSE & APPLICABILITY:**

Requires a research security program and related training for any research organization receiving over \$50M per year in Federal research funding

## **Research Security Program must cover:**

- ▶ Foreign travel security
- ▶ Research security training
- ▶ Cybersecurity
- ▶ Export Controls

## **Compliance:**

- ▶ Institutions must self-certify they meet the requirements as part of registration in SAM.gov
- ▶ Must maintain a description of the research security program on a publicly available website
- ▶ Designated research security point of contact with publicly accessible means to contact that individual

# International and Domestic Privacy Laws

## INTERNATIONAL
















137 countries have national privacy laws<sup>1</sup>

▶ Examples include:

- Global Data Protection Regulation (GDPR), **European Union**
- Personal Information Protection Law (PIPL), **China**
- General Data Protection Act (LGPD), **Brazil**
- Information Technology Act 2000 and SPDI Rules, **India**

## DOMESTIC

19 states have passed some form of privacy law<sup>1</sup>:

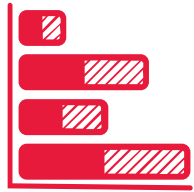
- |                                                                                                    |                                                                                                    |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
|  California (2) |  Indiana        |
|  Virginia       |  Delaware       |
|  Colorado       |  New Jersey     |
|  Connecticut    |  New Hampshire  |
|  Utah           |  Kentucky       |
|  Oregon         |  Nebraska       |
|  Texas         |  Maryland      |
|  Montana      |  Minnesota    |
|  Iowa         |  Rhode Island |
|  Tennessee    |                                                                                                    |

<sup>1</sup>According to the International Association of Privacy Professionals

# Challenges in the Current Landscape



# Challenges in the Current Landscape



## VOLUME

- ▶ Number of different rules to manage
- ▶ Huge amounts of data



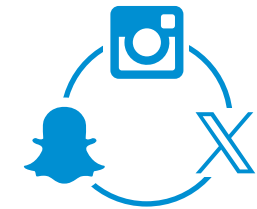
## LOCATION

- ▶ Decentralized computing environments
- ▶ Ability to accurately identify and categorize data



## GOVERNANCE

- ▶ Policies and procedures
- ▶ Training and awareness



## ENVIRONMENT

- ▶ Rules and tools continue to change



# Department of Education CUI Rule



# New Department of Education Proposed Rule

DUE OUT IN FALL OF 2024

*“The Department relies on schools participating in the federal student financial assistance programs and other grant programs under the Higher Education Act of 1965, as amended (HEA), to help carry out a wide range of business functions.*

*Schools routinely process, store, and transmit Controlled Unclassified Information (CUI), which includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and information.*

*The protection of sensitive data while residing in school information systems is of paramount importance to the Department.*

*To assure schools properly protect CUI, as required by Executive Order 13556, and the regulations at 32 CFR part 2002 which require non-Federal entities handling CUI to implement **NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171)**, the Department plans to propose to regulate on information security requirements.”*

The screenshot shows the Reginfo.gov website interface. At the top, there is a blue header with the seal of the Executive Office of the President and the text: "OFFICE of INFORMATION and REGULATORY AFFAIRS", "OFFICE of MANAGEMENT and BUDGET", "EXECUTIVE OFFICE OF THE PRESIDENT", and "Reginfo.gov". A search bar and navigation links for "Home", "Unified Agenda", "Regulatory Review", "Information Collection Review", "FAQs / Resources", and "Contact Us" are visible. The main content area is titled "View Rule" and includes links for "View EO 12866 Meetings", "Printer-Friendly Version", and "Download RIN". The rule details are as follows:

- ED/FSA: RIN: 1845-AA25, Publication ID: Spring 2024
- Title: Cybersecurity Standards for Institutions of Higher Education to Comply With EO 13556 and NIST 800-171
- Abstract: The Department relies on schools participating in the federal student financial assistance programs and other grant programs under the Higher Education Act of 1965, as amended (HEA), to help carry out a wide range of business functions. Schools routinely process, store, and transmit Controlled Unclassified Information (CUI), personally identifiable information (PII), sensitive personally identifiable information (SPII), and information. The protection of sensitive data while residing in school information systems is of paramount importance to the Department. To assure schools properly protect CUI, as required by Executive Order 13556, and the regulations at 32 CFR part 2002 which require non-Federal entities handling CUI to implement NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171), the Department plans to propose to regulate on information security requirements.
- Agency: Department of Education(ED), Priority: Other Significant
- RIN Status: Previously published in the Unified Agenda, Agenda Stage of Rulemaking: Proposed Rule Stage
- Major: Undetermined, Unfunded Mandates: Undetermined
- CFR Citation: None (To search for a specific CFR, visit the Code of Federal Regulations. ↗)
- Legal Authority: 20 U.S.C. 1090, 15 U.S.C. 6801 et seq., E.O. 13556
- Legal Deadline: None
- Timetable: A table with columns for Action, Date, and FR Cite. One entry is shown: NPRM on 10/00/2024.
- Regulatory Flexibility Analysis Required: Undetermined, Government Levels Affected: Undetermined
- Federalism: Undetermined
- Included in the Regulatory Plan: No
- RIN Data Printed in the FR: No

CLICK HERE ►

# 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
- ▶ 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)

# CUI and the Privacy Act

- ▶ Records containing personal details don't solely fall under the Privacy Act
- ▶ Such records may also be controlled under other categories and marked as CUI
- ▶ Deciding if certain personal information needs protection under the Privacy Act depends on the content of the information and the act's requirements
- ▶ Whether information is categorized or marked as CUI doesn't affect the decision to protect or release it under the Privacy Act







## What is CUI?

**Controlled Unclassified Information (CUI) refers to information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.**

- ▶ CUI is not classified, but it is still sensitive and warrants protection due to the potential impact of unauthorized disclosure
- ▶ It includes information that is related to national security, such as export control, critical infrastructure, or nuclear safeguarding information
- ▶ CUI is also applicable to information that involves privacy, such as personally identifiable information (PII), student records, or health information
- ▶ The goal of controlling CUI is to ensure such information is shared in a secure manner while maintaining compliance with applicable policies and legal requirements

<https://www.governmentattic.org/54docs/EDdirCUI2019.pdf>

# What is CUI?

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)



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://foiaexpress.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](mailto: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.

**CLICK HERE ▶**

# What would this rule require?

## LESSONS FROM THE DOD CUI RULE

### Defines 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 agency to handle using safeguarding or dissemination controls.

NARA Archives: Classification for CUI Categories

[CLICK HERE ▶](#)

FedRAMP-Moderate Equivalent Cloud Solutions

Provide “Adequate Security”  
NIST SP 800-171 Rev 2

System Security Plan (SSP)  
requirements **to be implemented**

Plan of Action and Milestones  
(POA&M) requirements **not yet  
implemented**

Create Incident Response  
Program

Report Cyber Incidents

Report Malicious SW Facilitate  
Damage Assessment



# CUI Category: Student Records

## STUDENT RECORDS

As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.

<https://www.archives.gov/cui/registry/category-detail/student-records>

## CUI Category: Student Records

**Banner Marking for Specified Authorities: CUI//SP-STUD**

**Banner Marking for Basic Authorities: CUI**

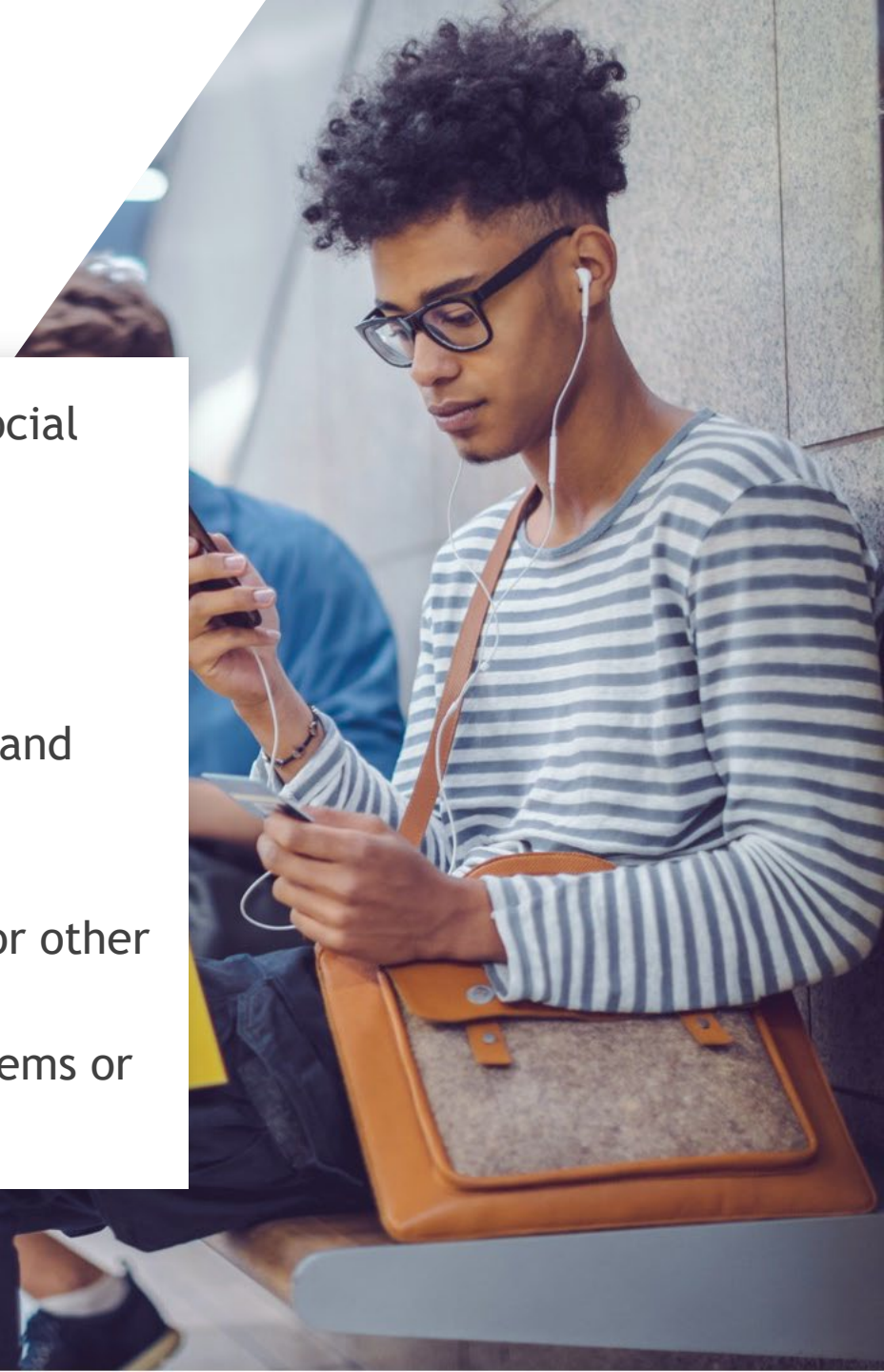
<b>Category Description:</b>	As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.		
<b>Category Marking:</b>	STUD		
<b>Alternative Banner Marking for Basic Authorities:</b>	CUI//STUD		
	<b>Safeguarding and/or Dissemination Authority</b>	<b>Basic or Specified</b>	<b>Banner Marking</b>
	<a href="#">20 USC 1232g(a)(1)(C)</a>	Basic	CUI
	<a href="#">25 CFR 43.14</a>	Basic	CUI
	<a href="#">25 CFR 43.22</a>	Specified	CUI//SP-STUD
	<a href="#">34 CFR 99.30(a)</a>	Basic	CUI
	<a href="#">34 CFR 99.31(a)(6)(ii)</a>	Basic	CUI
	<a href="#">34 CFR 99.33(a)(1)</a>	Basic	CUI



## CUI EXAMPLES

# Student Information

- ▶ Personally identifiable information (PII), such as student names, social security numbers, and dates of birth
- ▶ Educational records, including grades, test scores, and transcripts
- ▶ Health information, such as immunization records and details of disabilities or accommodations
- ▶ Financial information, like tuition payments, financial aid details, and loan data
- ▶ Disciplinary records and any associated notes or documentation
- ▶ Information relating to a student's eligibility for veteran benefits or other specialized programs
- ▶ Online identifiers and account details used within educational systems or platforms





## Safeguarding

- ▶ Safeguarding aims to prevent unauthorized individuals from accessing CUI (Controlled Unclassified Information)
- ▶ If not stored in Federal information systems, CUI must be stored in locked places such as offices, drawers, and file cabinets
- ▶ Extra caution is needed in private offices cleaned or maintained after hours
  - Secure CUI in locked desks or file cabinets
- ▶ If you work with specified CUI categories like Sensitive Security Information, follow both the outlined safeguarding standards in relevant laws, regulations, and policies as well as this directive
- ▶ Do not expose CUI to others who don't have lawful government purpose to see it
- ▶ Use a standard form (SF 901) cover sheet to protect CUI from casual viewing
- ▶ Secure CUI in a locked area when leaving the vicinity

<https://www.governmentattic.org/54docs/EDdirCUI2019.pdf>

# Scoping the Environment



# Microsoft 365 Government (DoD)

	Microsoft 365 "Commercial"	Microsoft 365 Government (GCC)	Microsoft 365 Government (GCC High)	Microsoft 365 Government (DoD)
Customer Eligibility	Any customer	Federal, SLG, Tribes, Eligible Contractors (DIB, FFRDC, UARC)	Federal, Eligible Contractors (DIB, FFRDC, UARC)	<b>DoD only</b>
Region / Geo Locations	US & OCONUS	CONUS Only	CONUS Only	<b>CONUS Only</b>
FedRAMP	No	Moderate ATO & High <sup>1</sup>	<b>Moderate<sup>1</sup> &amp; High<sup>1</sup> equivalency</b>	
DFARS 252.204-7012	No	Yes	Yes	<b>Yes</b>
FCI + CMMC L1	Yes <sup>^</sup>	Yes	Yes	<b>Yes</b>
CUI / CDI + CMMC L2-3	No	Yes <sup>^ ^</sup>	Yes	<b>Yes</b>
ITAR / EAR / NOFORN	No	No	Yes	<b>Yes</b>
DoD CC SRG Level	No	IL2 PA	IL4 <sup>2</sup>	<b>IL5 PA</b>
NIST SP 800-53 / 171 <sup>3</sup>	Yes <sup>4</sup>	Yes	Yes	<b>Yes</b>
CJIS Agreement	No	State	Federal	<b>No</b>
NERC / FERC	No	Yes <sup>^ ^</sup>	Yes	<b>Yes</b>
Customer Support	Worldwide / Commercial Personnel		<b>US-Based / Restricted Personnel</b>	
Directory / Network	Azure Public "Commercial"		<b>Azure Government</b>	
			<b>US Sovereign Cloud</b>	

<sup>1</sup> Equivalency, 3PAO SAR for High Impact Level; Supports accreditation at noted impact level

<sup>2</sup> Equivalency, PA issued for DoD only

<sup>3</sup> Organizational Defined Values (ODV's) will vary

<sup>4</sup> Insufficient to demonstrate equivalency IAW DoD Memo dated 21 Dec 2023

<sup>^</sup> M365 Commercial Cloud is not intended for Government requirements

<sup>^^</sup> CUI Specified (e.g., ITAR, Nuclear, etc.) not suitable; requires US Sovereignty



Lessons learned from the DoD:  
**Not all platforms are compliant with CUI.**

<https://techcommunity.microsoft.com/t5/public-sector-blog/understanding-compliance-between-commercial-government-dod-amp/ba-p/4225436>

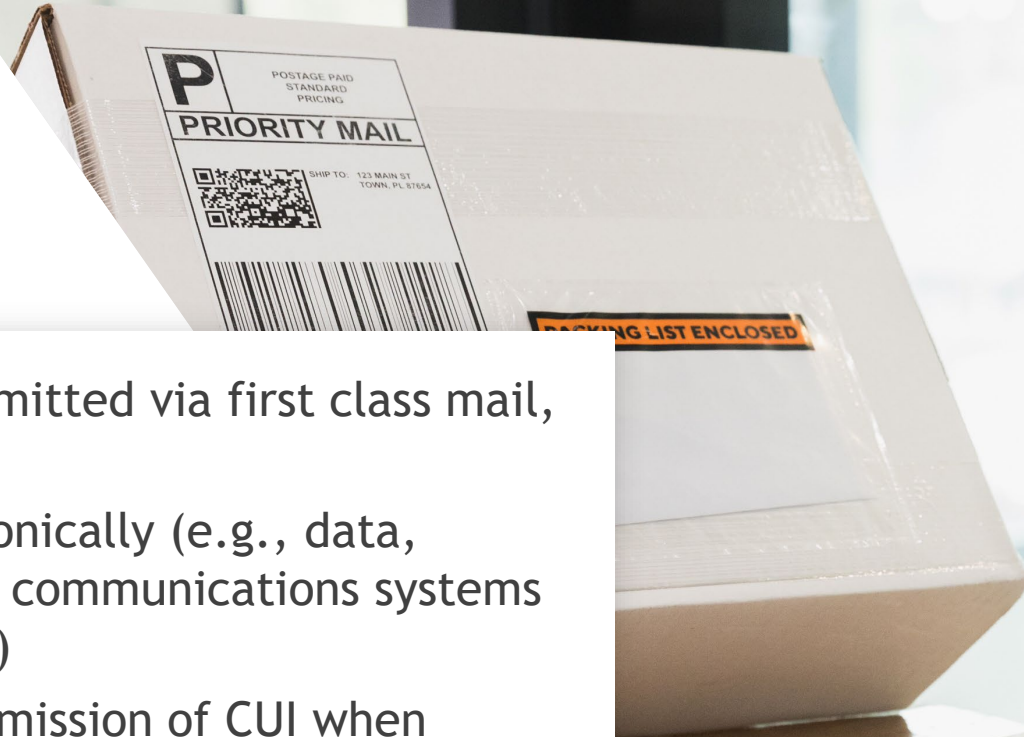
# Safeguarding, Destruction & Decontrol





# CUI Transmission

- ▶ CUI and material may be transmitted via first class mail, parcel post, or bulk shipments
- ▶ CUI may be transmitted electronically (e.g., data, website, or e-mail), via secure communications systems or systems (using PKI, SSL, TLS)
- ▶ Avoid wireless telephone transmission of CUI when other options are available
- ▶ CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission





# Physical & Logical Safeguarding

## PHYSICAL

- ▶ All CUI information will be protected in accordance with the requirements under the Basic level of safeguard and dissemination.
- ▶ During working hours, take steps to **minimize the risk of access by unauthorized personnel**, such as not reading, discussing, or leaving CUI unattended where unauthorized personnel are present. The use of CUI coversheets, as mentioned earlier, is optional.
- ▶ After working hours, store Information in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

## LOGICAL

- ▶ Data must be encrypted when:
  - Data At Rest
  - Data In Use
  - Data In Transit
- ▶ Includes types:
  - FIPS 140-2, 140-3
  - VPN/IPsec
  - Encryption Keys
  - PKI/Certificates

# Destruction of CUI

## 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

- ▶ Destruction method must make CUI **unreadable, indecipherable, and irrecoverable**
- ▶ CUI may not be placed in office trash bins or recycling containers

## Two approved methods for destruction of CUI:

**BONUS METHOD:**  
Using any destruction techniques approved for classified national security information

- 1 Cross-cut shredding that produces 1 1/2" x 3/8" particles (or smaller)
- 2 Pulverizing
- 3 Incineration

# Decontrol



- ▶ When protection is no longer needed, information should be removed from under the CUI program ASAP
- ▶ CUI decontrol can happen automatically under certain conditions or through a decision by the designator
- ▶ Conditions for automatic decontrol include:
  - a) No longer needing control by law,
  - b) A decision to disclose to the public,
  - c) Disclosure under an access statute, or
  - d) When a specific event or date occurs
- ▶ A designator can also decide to decontrol CUI in response to a request or in conjunction with a declassification action
- ▶ Each agency can set its own rules about who can decontrol CUI, as long as they are consistent with law and policy

# Self-Inspection Program and Marking



# CUI Self-Inspection Program

- ▶ The CUI Self-Inspection Program will be implemented by ED and are required to be carried carry out **annually**
- ▶ The purpose of these self-inspections is to evaluate program effectiveness, monitor compliance level, and track the progress of CUI implementation
- ▶ The CUI Program Manager will provide formats for documenting self-inspections, recording findings, and advice for addressing deficiencies and implementing remedial actions
- ▶ The results of these reviews must be reported to the ED CUI Program Manager
- ▶ The self-inspections will also extend to contractor companies under the offices' supervision
- ▶ The overall results from department-wide self-inspections will be used to further refine and improve the CUI Self-Inspection Program



# Markings Handbook and Other Resources



**DIRECT LINK TO THE  
MARKING HANDBOOK**



The CUI Markings Handbook is available on the CUI Executive Agent [website](#) along with additional resources, such as [CUI Coversheet \(SF 901\)](#), link to how to purchase [Media Labels \(SF 902 and SF 903\)](#) from GSA, and [Destruction Equipment Labels](#).

# CUI

## ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

## ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 91 (11-18)  
Prescribed by GSA/ISOO | 32 CFR 2002

# CUI

		CONTROLLED UNCLASSIFIED INFORMATION
<b>This equipment has been approved for the destruction of <i>Controlled Unclassified Information (CUI)</i>.</b>		
Inspected and Approved by:	Date:	Serial Number:
<input type="text"/>	<input type="text"/>	<input type="text"/>
		Make/Model:
		<input type="text"/>
<small><b>Note:</b> Only equipment which produces particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller) may be approved. Please direct any questions to:</small>		

This medium is  
**CUI**  
U.S. Government Property

SF 903 (11-18)

This medium is  
**CUI**  
U.S. Government Property

SF 902 (11-18)

Protect it from unauthorized  
disclosure in compliance with applicable  
executive orders, statutes, and regulations.





# Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > CUI Categories



[Use the CUI logo](#)

[Contact Us](#)

[Contact an Agency](#)

[About CUI](#)

[CUI History](#)

[FAQs](#)

[CUI Registry](#)

[Categories](#)

[CUI Markings](#)

[Limited Dissemination](#)

[Controls](#)

[Decontrol](#)

[Registry Change Log](#)

[Policy and Guidance](#)

[Glossary](#)

[CUI Reports](#)

[CUI Training](#)

## CUI Categories

\*\*\*\*\* IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT \*\*\*\*\*

Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.

Search the Registry

## CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

**Organizational Index Grouping**

**CUI Categories**

Questions?





**CONTACT US** ▶

### About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

For more information, please visit: [www.bdo.com](http://www.bdo.com).

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2024 BDO USA, P.C. All rights reserved.

