Welcome!

Best Practices/Emerging Trends:

- Export Controls & Restricted Parties
- Data and Information Security
- Controlled Unclassified Information
- Conflict of Interest & Foreign Influence

MONTANA STATE UNIVERSITY

Today's Speakers

- **Quinton King** – Export Control Officer, Montana State University
- **Zach Scott** – Associate VP for Research Compliance and Technology Transfer, University of Montana
- **Justin Van Almelo** – Chief Information Security Officer and Research Chief Information Officer, Montana State University
- **John White** – Information Systems Security Manager, Montana State University
- **Daniella McGuire** – Conflict of Interest Manager, Montana State University

MONTANA STATE UNIVERSITY

Disclaimer

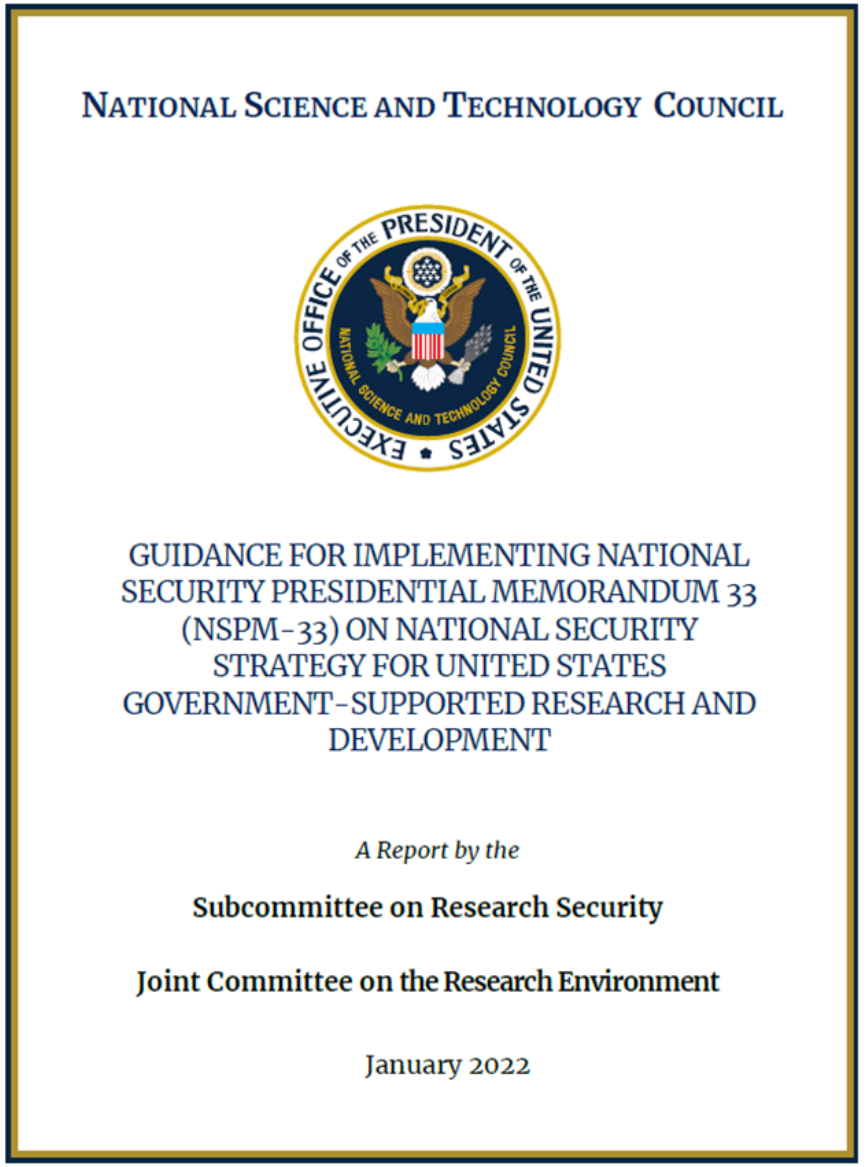
The opinions expressed are those of the presenters and may not necessarily reflect Montana State University or the University of Montana.

MONTANA STATE UNIVERSITY

Emerging Trends . . .

National Security Presidential Memorandum 33 (NSPM-33)

- Response to concerns of foreign misappropriation of US Federally-funded research and intellectual property.
- Includes several requirements:
  - Adoption of “Digital Persistent Identifiers” for researchers
  - Standardized Conflict of Interest/Conflict of Commitment disclosures
  - Development of appropriate consequences for disclosure violations
  - Funding Agency information sharing for disclosure violations
- Additional Research Security Program requirement for “Covered Research Organizations” (i.e. those receiving >$50M in annual Federal S&E research funding) covering:
  - Cybersecurity
  - Foreign Travel Security
  - Research Security
  - Export Control Training



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

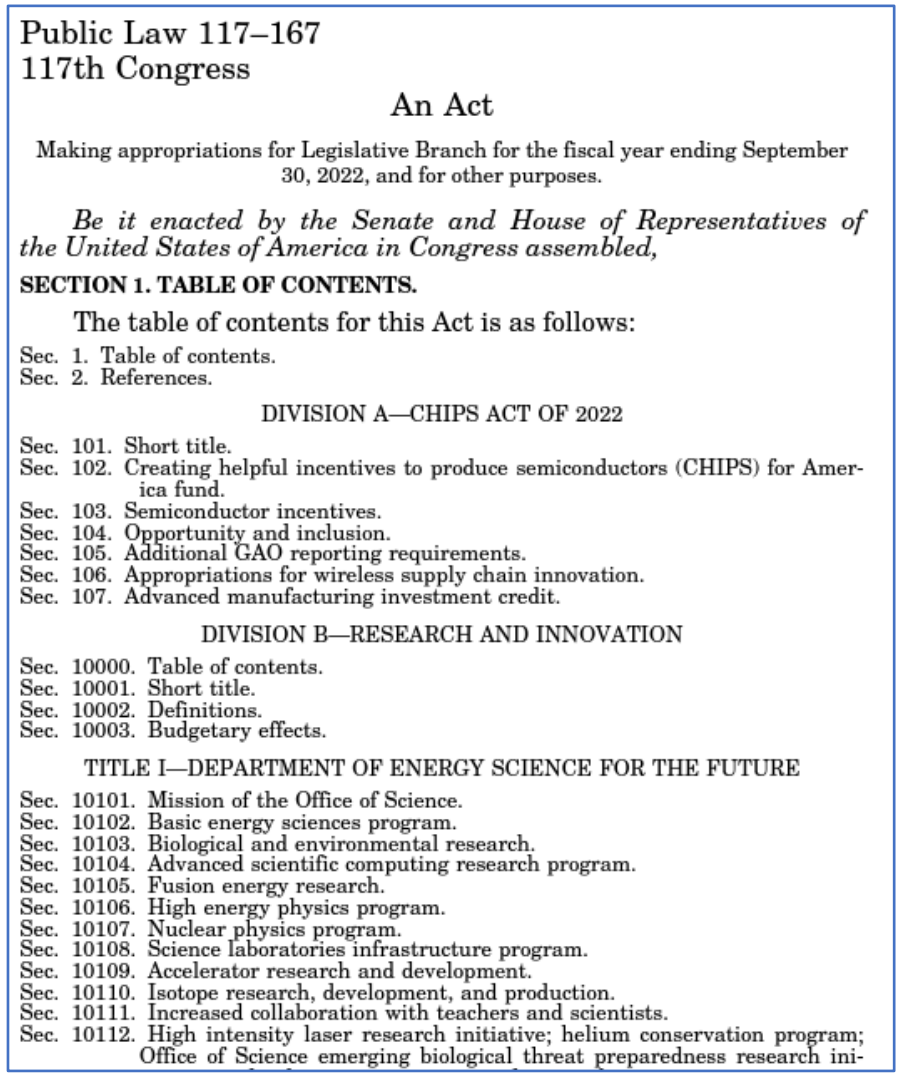
Joint Committee on the Research Environment

January 2022

Emerging Trends . . .

CHIPS and Science Act

- Response to concerns of dependence on foreign-produced semiconductors and malign foreign influence in US Federally-funded research.
- Cross-references and works in tandem with NSPM-33.
- Includes a number of Research Security Training requirements for “Covered Individuals” (those who will substantively contribute to a Federally-funded research project), including:
  - Cybersecurity
  - International Collaboration and Travel
  - Malign Foreign Interference
  - Conflict of Interest and Conflict of Commitment
- Includes a requirement that, upon agency request, institutions seeking Federal awards report employee engagements with foreign entities (contracts, appointments, etc.).
- Includes an institutional disclosure requirement for financial support >$50K from a “foreign country of concern” (China, North Korea, Russia, Iran).



Public Law 117–167
117th Congress

An Act

Making appropriations for Legislative Branch for the fiscal year ending September 30, 2022, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Emerging Trends . . .

Evolving Geopolitical Landscapes

- US policy makers routinely use economic sanctions and export controls to respond to world events . . .
- Can potentially impact collaborations with certain foreign researchers and institutions
- Can potentially impact engagements with certain foreign vendors

Emerging Trends . . .

State of Montana HB 946

- HB 946 passed in the most recent legislative session, signed by Governor Gianforte on May 22, 2023
- Includes a reporting requirement for “all existing collaborations, partnerships, contracts, donations and contributions related to an entity or individual associated with a foreign country of concern.” (i.e. China, North Korea, Russia, Iran).

AN ACT IMPLEMENTING THE PROVISIONS OF HOUSE BILL NO. 2; PROVIDING FOR REPORTS TO THE EDUCATION INTERIM BUDGET COMMITTEE FROM THE MONTANA STATE LIBRARY, THE OFFICE OF THE COMMISSIONER OF HIGHER EDUCATION, AND THE OFFICE OF PUBLIC INSTRUCTION; REVISING EDUCATION LAWS RELATED TO EARLY EDUCATION AND KINDERGARTEN; ESTABLISHING UNDER WHAT EXCEPTIONAL CIRCUMSTANCES A SCHOOL DISTRICT MAY ADMIT STUDENTS OUTSIDE REGULAR AGE PARAMETERS; CLARIFYING THAT KINDERGARTEN IS A SINGLE-YEAR PROGRAM; PROVIDING THAT THE EDUCATION INTERIM BUDGET COMMITTEE DIRECT A STUDY RELATED TO SERVICES PROVIDED BY THE DEPARTMENT OF ADMINISTRATION; PROVIDING DEFINITIONS; AMENDING SECTIONS 20-5-101 AND 20-7-117, MCA; AND PROVIDING AN EFFECTIVE DATE AND AN APPLICABILITY DATE.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

Section 3. Office of commissioner of higher education reports.

(4) (a) The office of the commissioner of higher education shall report to the education interim budget committee provided for in 5-12-501 on all existing collaborations, partnerships, contracts, donations, and contributions related to an entity or individual associated with a foreign country of concern. The first report must be made by July 31, 2023. Following the first report, the office of the commissioner of higher education shall report twice more during the following year, by January 31 and July 31.

(b) The report required in subsection (4)(a) must include the following information:

(i) a description of each partnership, collaboration, contract, donation, or contribution;

(ii) the goal of the partnership, collaboration, contract, donation, or contribution;

(iii) the length of the partnership, collaboration, contract, donation, or contribution;

(iv) whether the arrangement is curriculum oriented or research oriented;

(v) the full legal name of the individual or entity that made or received the contribution or donation

Emerging Trends . . .

- **New compliance requirements?**
- **Formalization of previously recognized obligations?**
- **Renewed focus on enforcement . . .**

Emerging Trends . . .

Compliance Management

Feds hit Penn State University with false claims lawsuit over cyber compliance

Derek B. Johnson September 14, 2023

Students between class, Penn State University. A lawsuit lawsuit represents one of the first attempts by the government to hold contractors accountable for false cybersecurity claims made in federal contracts. (Photo by John Greim/LightRocket via Getty Images)

The United States government is bringing legal action against Penn State University under the False Claims Act, saying the university lied or misled about its adherence to government cybersecurity protocols when contracting with the federal government.

PRESS RELEASE

Ohio State University Pays Over $875,000 to Resolve Allegations that It Failed to Disclose Professor's Foreign Government Support

Thursday, November 10, 2022

Share

For Immediate Release

Office of Public Affairs

The Ohio State University (OSU), a public university in Columbus, Ohio, has paid $875,689 to resolve civil allegations that it failed to disclose an OSU professor's affiliations with and support from a foreign government in connection with federal research funding.

February 10, 2021

Princeton Penalized for Alleged Research-Related Export Violations

LinkedIn Facebook Twitter Send Embed

BASS BERRY + SIMS
CENTERED TO DELIVER.

On February 1, the U.S. Commerce Department, Bureau of Industry & Security (BIS), announced a settlement (available here) with Princeton University in connection with 37 alleged violations of the Export Administration Regulations (EAR). The EAR are the main regulations that govern exports of commercial goods, software and technology; BIS has principal responsibility for administering and enforcing the EAR.

The settlement is a valuable reminder of the amount of export-controlled activity that takes place at and involving universities, academic medical centers, and other research institutions. Penalties for export violations can be significant. Legal departments, compliance departments, and offices of sponsored research therefore must ensure that faculty – many of whom may be non-U.S. nationals – are aware of their responsibilities under U.S. export law.

WRITTEN BY:

Bass, Berry & Sims PLC Contact + Follow

Thaddeus McBride + Follow

PUBLISHED IN:

Bureau of Industry and Security (BIS) + Follow

Export Administration Regulations (EAR) + Follow

Export Controls + Follow

Exports + Follow

Settlement + Follow

Best Practices . . .

1. **Zach – Export Controls**
2. **Justin – Cybersecurity**
3. **John – CUI**
4. **Daniella – COI/COC**
5. **A couple hypotheticals . . .**
6. **Q&A**

University of Montana
Office of Research and Creative Scholarship

Zach Scott, PhD, JD
Assoc. VP for Research Compliance and Tech. Transfer

What are export control laws?

The term “export controls” means the federal laws and regulations that control the distribution to foreign nationals and foreign countries of items, services, technology, and software. Depending on the circumstances, advance authorization (i.e., license) from the US government to engage in such exchanges may be required. In other cases, the exchange may be prohibited.

Designed to advance U.S. foreign policy goals, prevent transfer of sensitive military or dual-use technologies to adversaries, and to fulfill international treaty obligations.

Whether a license is required in any of these circumstances would depend on three factors: (1) the nature of the item/service/technology/software; (2) the country of destination; and (3) the end user of the item.

There are substantial penalties for noncompliance with export control laws:

- Criminal violations: $50,000-$1,000,000 or five times the value of the export, whichever is greater per violation (range depends on the applicable law), up to 10 years imprisonment.
- Civil penalties: loss of export privileges, fines $10,000-$120,000 per violation.
- Puts federal funding at risk -- for the university and for the individual.

Main U.S. Government Agencies

Department of Commerce
Bureau of Industry and Security (BIS)
Export Administration Regulations (EAR)

Department of State
Directorate of Defense Trade Controls (DDTC)
International Traffic and Arms Regulations (ITAR)

Department of Treasury
Office of Foreign Assets and Control (OFAC)

Export Administration Regulations (EAR) Basics

- **“Dual-use” and military-use items**

- **“Items”**
  - Physical commodities
  - Technology
  - Software

- Commerce Control List (CCL)
- Classification: EAR99 or specific ECCN

International Traffic in Arms Regulations (ITAR) Basics

- **Military-use items and services**

- **“Items”**
  - Physical commodities
  - Technology
  - Software
  - “Defense services”
  - Nanotechnology, new materials, sensors

- United States Munitions List (USML)

Office of Foreign Assets Control (OFAC) Basics

Sanctioned Countries

- Country-specific restrictions
- Not just financial transactions
- Focus on end-user, not the technology
- Specific license vs general license
- Denied Parties Lists/Restricted Party Lists (BIS, DDTC, and OFAC)
- Use Consolidated Screening List

Cuba, Iran, Syria, North Korea, Ukraine/Russia-Related, and More

Deemed Exports

The disclosure or transfer of export-controlled software, technologies or technical data to a foreign entity or individual *inside* the US is “deemed” to be an export to the home country of the foreign entity or individual.

Applies to technology transfers under the EAR and the provisions of ITAR technical data and defense.

A “deemed export” license may be required.

Applies regardless of role: graduate students, post-docs, visiting scholars, and faculty.

Fundamental Research Exclusion (FRE)

- The term *Fundamental Research* means " basic and applied research in science and engineering, *the results of which ordinarily are published and shared broadly within the scientific community"*, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." A university's research normally will be considered as fundamental research unless the university or its researchers accept sponsor restrictions on publication of scientific and technical information resulting from the project or activity.
- Conducting fundamental research is key to maintaining an environment of openness in an academic setting.
- The FRE applies only to the exchange of research data and information, not to the transmission of tangible goods.
- The FRE is destroyed if the university accepts any contract clause that:

  Forbids the participation of foreign persons;

  Gives the sponsor a right to approve publications resulting from the research; or

  Otherwise operates to restrict participation in research and/or access to and disclosure of research results.

Key Takeaways

- American IHE are coming under increased scrutiny for compliance with export control laws.
  - Complex series of laws and regulations – not always harmonious.
- Determination of liability and compliance requires a case-by-case analysis by IHE export control officer.
  - Come early – export control licensing process can take many months.
- IHE take advantage of fundamental research exclusion.
  - Watch for publication restrictions from sponsors and collaborators.

Research Data Security

Justin van Almelo

CISO | Research CIO – Montana State University

Know Your Data

- Who defines the categories of research data?
- What categories of research data are you working with?
- What compliance requirements do those data have?
- Where is your data backed up?

Know Your Infrastructure

- What storage options are available?
- What storage options are appropriate?
- How are unique requirements assessed?
- Securing unique requirements.

Know Your Resources

Security – Not Just For Confidential Data

- Confidentiality
- Integrity
- Availability

MONTANA STATE UNIVERSITY

JOHN WHITE

CONTROLED UNCLASSIFIED INFORMATION (CUI)

AGENDA

- **Discuss the following topics:**
- What is CUI?
- Who Decides?
- Mark and Label CUI
- Dissemination / Sharing
- Destruction
- Wrap Up

What is CUI?

- **CUI is generally government-created or owned information** that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.
- **Anyone can be an Information Owner** and create CUI as long as it is generated for, or on behalf of, an Executive Branch agency under a contract and it falls into one of the over one hundred DOD CUI categories. However, in most situations, Industry will be guided by its customer (the Information Owner) on what is CUI and what isn't.
- **CUI is not a classification** and should not be referred to as "classified as CUI." A better way to phrase it is "designated as CUI."
- **CUI is not corporate intellectual property**, unless created for or included in requirements related to a Government contract. Contractors should consult with their Government Contracting Activity (GCA) to make this determination.
- **Access to CUI is based on having a lawful government purpose** which is similar to the need-to-know concept for access to classified or FOUO type information but intentionally less stringent.
- Material ***cannot be marked CUI*** in order to:
  - Conceal violations of the law, inefficiency, or administrative errors.
  - Prevent embarrassment to a person, organization, or agency.
  - Prevent open competition.

WHAT IS *NOT* CUI?

- Classified information or a classification
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publicly available information

WHO DECIDES?

The **Information Owner (IO)** of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the IO is responsible for applying the appropriate CUI markings and dissemination controls accordingly.

Information Owners include:

- DoD civilian and military personnel
- Agencies
- Contractors providing support to the DoD pursuant to contractual requirements

MARK/LABEL Emails with CUI

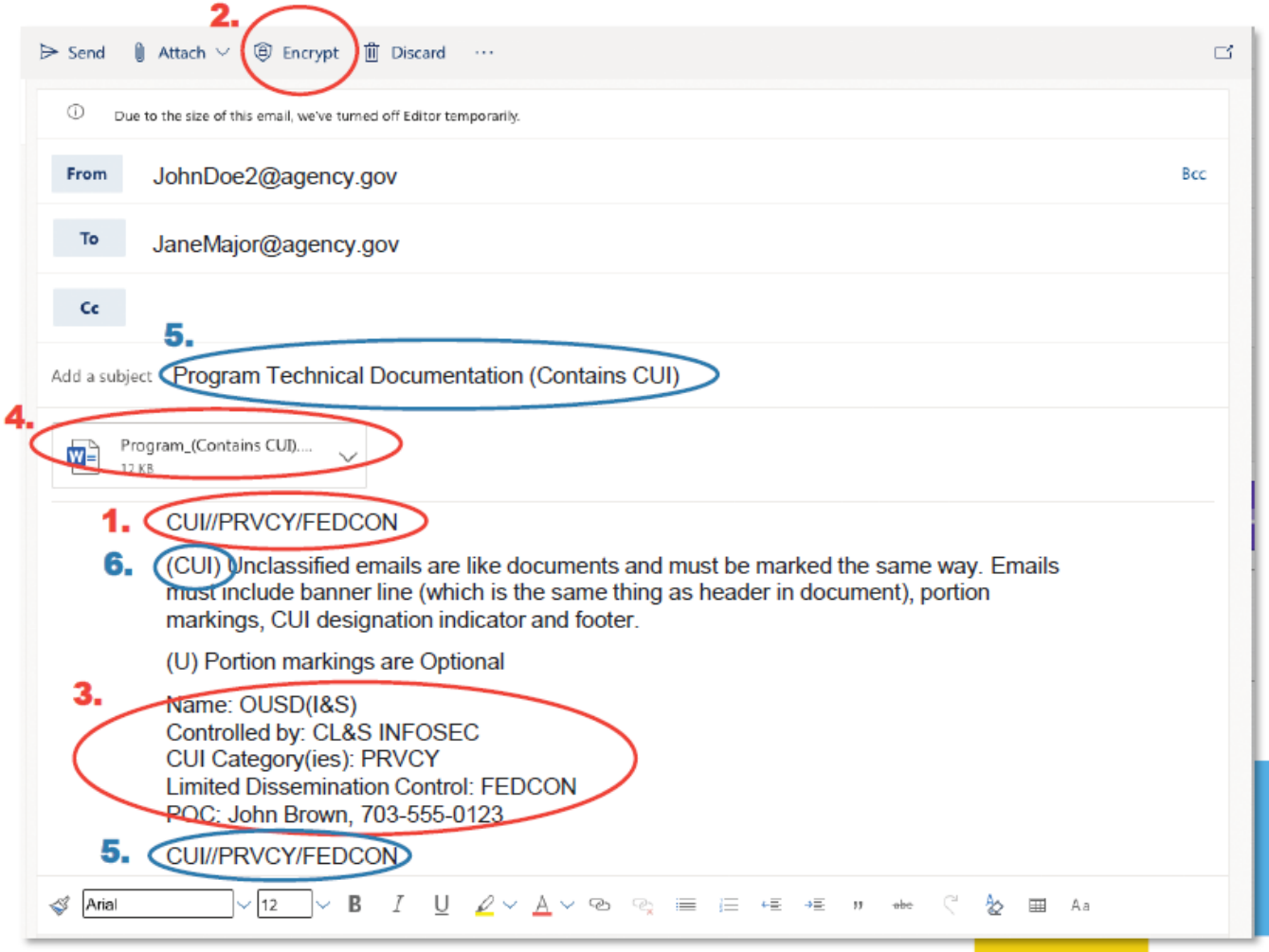
Required

1. Must apply "CUI" to top/banner.
2. **Must be encrypted.**
3. Must contain a CUI *Designation Indicator* block.
4. If including attachments containing CUI, file name must indicate it includes CUI.

Optional but best practice

5. Apply "CUI" to footer and subject line.
6. All paragraphs known to contain CUI may be portion marked.

DO NOT USE PERSONAL EMAIL ACCOUNTS to send CUI. This is necessary to ensure proper accountability for Federal records and to facilitate data spill remediation in accordance with Public Law 113-187 and the January 16, 2018 Deputy Secretary of Defense memorandum.



MARK/LABEL

Marking Media

- Removeable media and storage devices containing CUI must be marked.
- Standard Form 902 (stickers) are available through GSA for purchase but only the Government can order them. Find out more here.
- You can also create your own stickers. Find out more here.
- It is recommended you always engage with your **Information Owner** for additional guidance on what is required to be marked for your program (systems, materials etc.).

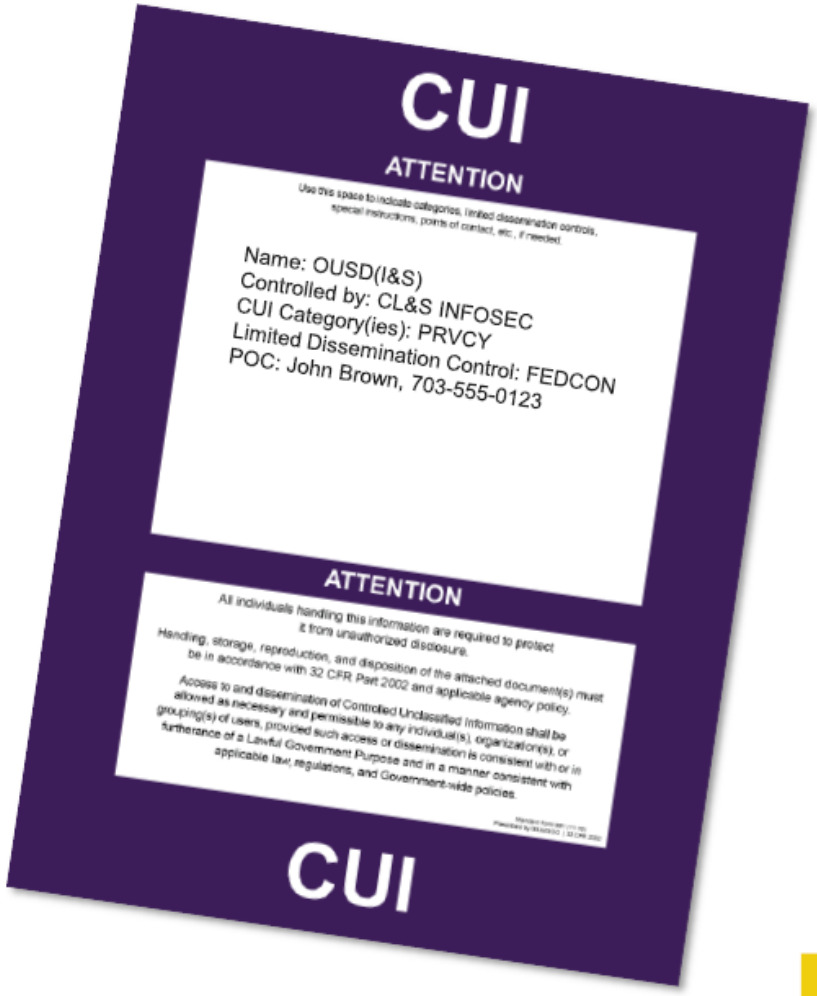
References:

- ISOO marking guidebook for more information https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf
- 32 CFR 2002 https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

MARK/LABEL

CUI Coversheets (Optional)

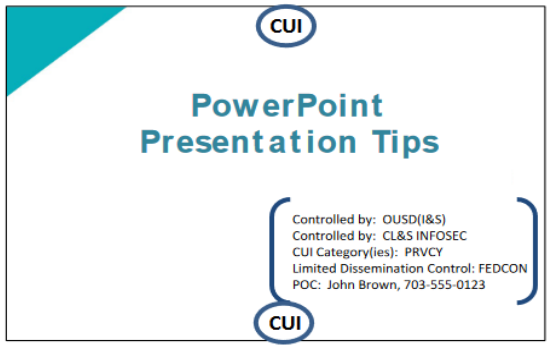
- First blank area of coversheet CAN be filled out with Designator indicator.
- You can download a copy of the CUI coversheet (SF901) at either of these sites:
  - https://www.gsa.gov/forms-library/controlled-unclassified-information-cui-coversheet-0
  - https://www.archives.gov/cui/additional-tools

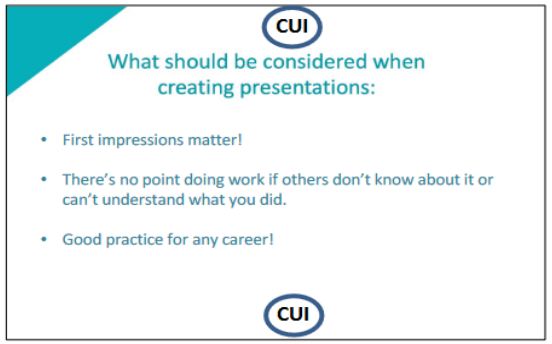


Mark and Label PowerPoint Presentations and Documents

CUI Markings for Unclassified Documents

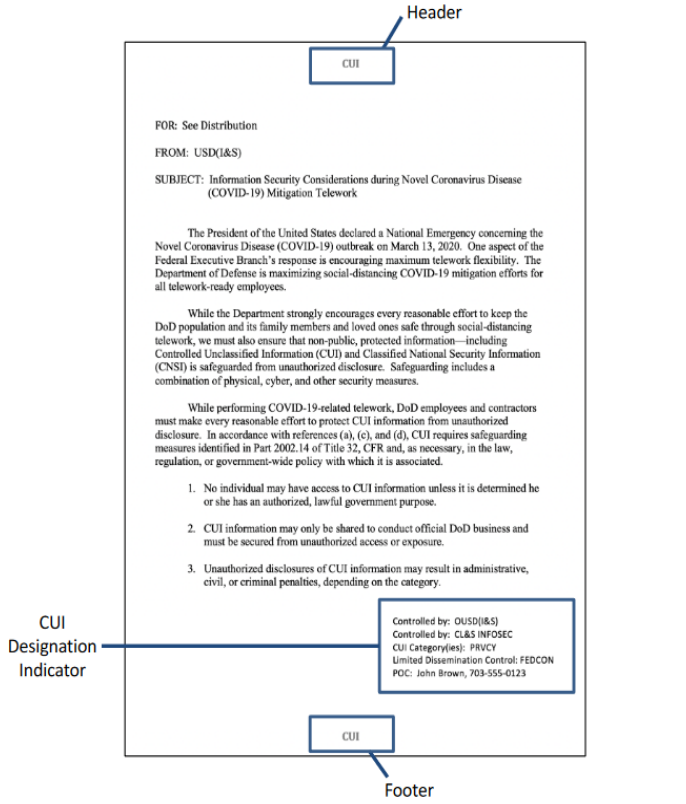
Example of markings on a CUI slide presentation without portion markings.





CUI Markings for Unclassified Documents

Example of markings on a CUI document without portion markings.



CUI is limited to those with a lawful Government purpose.

A lawful Government purpose is 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).

DISSEMINATE

Sharing CUI

IN PERSON

- Ensure you are in a controlled area where you cannot be overheard, recorded etc.

ELECTRONIC TRANSMISSION

- Must apply "CUI" to top/banner.
- **Must be encrypted.**
- Must contain a CUI *Designation Indicator* block.
- If including attachments containing CUI, file name must indicate it includes CUI.
- DO NOT USE PERSONAL EMAIL to transmit CUI.
- There are available Secure File Transfer Protocol (SFTP) sites (i.e. SAFE site). Always check with your customer on which sites you are able to use.

FAX

- Sender is responsible for determining appropriate protections are in place at the receiver end and Fax machine is located in a controlled government facility. Sender should contact receiver to inform them CUI is being transmitted.

MAIL

- May be transmitted via first class mail, parcel post, or bulk shipments. Do not place CUI markings on the outer envelopes or packaging when mailing.
- 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.
- Remember to track the package.

When to share CUI?
When access promotes a common project or operation between agencies or under a contract or agreement with the designating agency, then share!

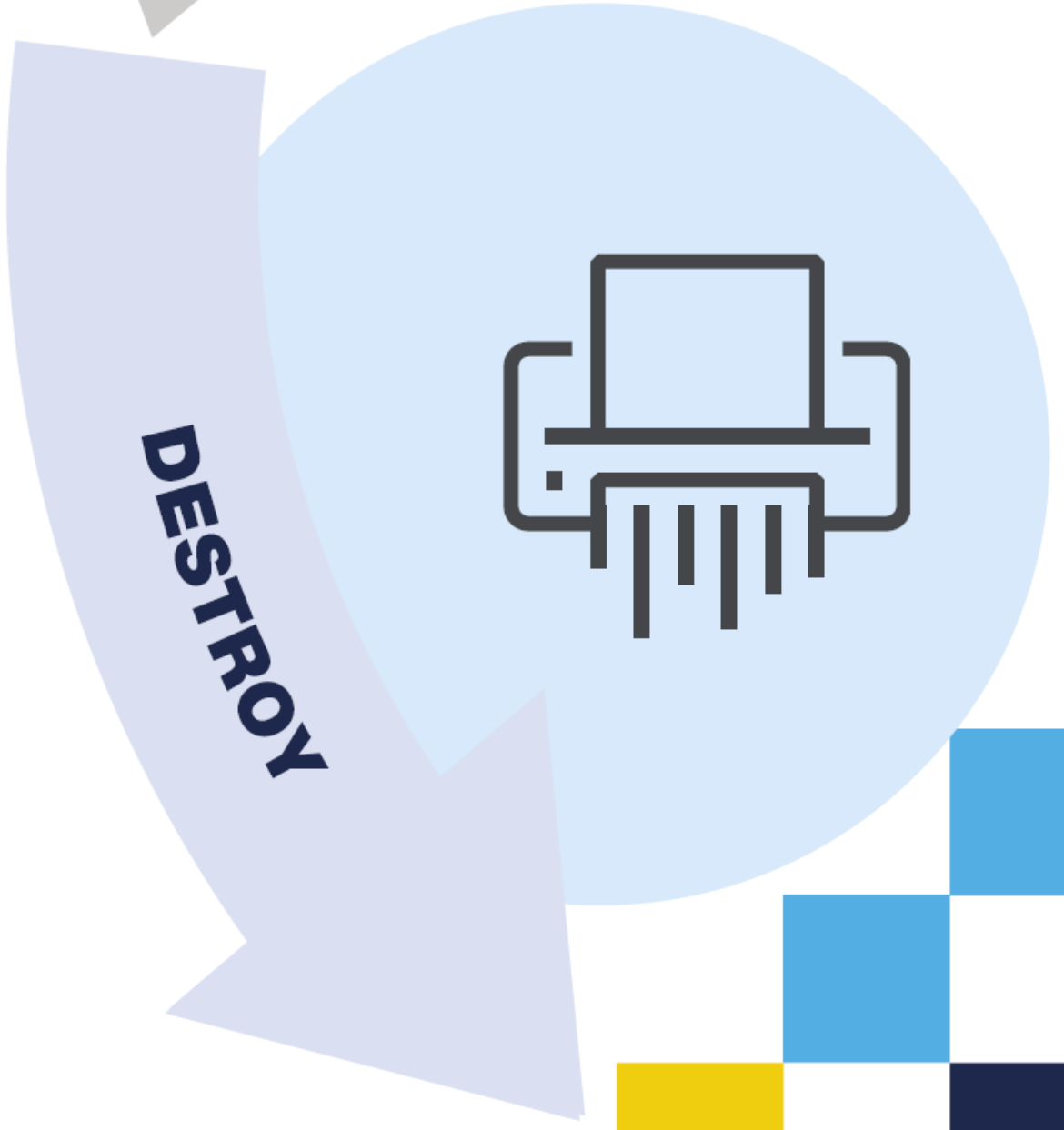
When NOT to share CUI?
If access harms or inhibits a common project or operation between agencies or under a contract or agreement with the designating agency, then do not share.

CUI should be destroyed or decontrolled whenever possible to reduce risk of exposure to unauthorized individuals.

Employees and contractors should contact the **Information Owner** to discuss decontrolling (downgrading) the CUI material when the need arises.

Triggers to request decontrol may include:

- Request to release the CUI material to the public
- End of contract
- Contract Renewal



WRAP UP

1. National Security is affected by the loss of CUI and we must protect it.
2. **The FIRST thing you should do is work with the Information Owner (customer, prime, agency, GCA etc.)** to validate CUI requirements.
3. Understandings of the NARA and DoD registries are paramount. Get familiar with them!
4. Stay in the know! Continue to look for updates to the CUI program.
5. Failure to comply with CUI requirements may result in administrative or criminal sanctions, fines and penalties.

Conflict of Interest

What all employees need to know

- *The Mission of MSU is enhanced by the sustained, active interaction of members of the University Community with*
  - *Business*
  - *Government*
  - *Not-for-profit groups*
  - *Professional societies*
  - *Academic Institutions, and*
  - *Other individuals and organizations*

Conflict of Interest

However, these interactions and other activities can create the potential for conflict of interest in which University employees' external and internal activities or interests COULD influence, or appear to influence, the manner and extent to which those individuals carry out their University responsibilities.

Common Types of Conflicts

1. Relatives and Personal Relationships
2. Financial
3. Foreign Influence
4. Commitment (time spent away from MSU that conflicts with work time)
5. Intersections

Common Examples

- Supervising a spouse
- Performing work for another company during work hours or using MSU property (i.e. computer or phone).
- Initiating a contract in which a family member can benefit.
- Accepting gifts or benefits from a contractor related to job duties at MSU.
- Proposing that MSU enter a contract with a company in which an employee has ownership or could gain from financially.
- Serving on a search committee when a relative is in the applicant pool.
- Owning part of a business that sells goods or services to MSU.
- Consulting for an outside entity.
- Funding received from any foreign government or entity or participation with a foreign talent program.
- Employing students or other employees outside of the University.
- Accepting Academic appointments while on leave from MSU or obtaining brief transitional appointments.

So what can't we do?

1. Use confidential MSU information for private benefit
2. Acquire a business interest [via MSU] for private benefit
3. Use MSU resources for private work
4. Make a contract decision at MSU when already involved on the private side of that contract

What do I do If I THINK I might have a Conflict?

Consult with the Office of Research Compliance. COI is common and can be managed In most cases. Keep in mind that COI protects YOU and the University.

Office of Research Compliance
114 Lewis Hall
406-994-6998
Kirk.Lubick@montana.edu

Or visit: www.montana.edu/orc/conflict-interest/

ONCE COI HAS BEEN DISCLOSED

- Meet with COI Manager to discuss perceived conflict;
- Work with COI Manager to draft a COI Plan that provides guidance on managing the conflict;
- COI Committee provides feedback regarding plan and votes to approve.

Hypothetical 1 . . .

A researcher at your institution specializing in AI/ML announces they are planning to travel to China to present at an academic conference hosted at a Chinese university. They will then be collecting/analyzing some data with a collaborator at that university.

Hypothetical 2 . . .

A US Air Force-funded researcher specializing in advanced radar and energy absorbing materials has been approached by a US-based subsidiary of a Finnish company seeking to collaborate. Company wants to sponsor research at the university relating to solar energy, but also wants the researcher to agree to provide consulting services on other related projects. Company is requesting that all conversations and any research outcomes be kept confidential, with no publications unless the company approves of the content.

Q&A

Thank You!