GEN501: Protection of Sensitive Information

September 2023

GEN501: Protection of Sensitive Information

The Department of Energy (DOE), Office of Science (SC), does not authorize the Thomas Jefferson National Accelerator Facility (hereafter TJNAF or Jefferson Lab) or Jefferson Science Associates LLC, (JSA) to receive, store, transmit, or originate classified information as defined under Executive Order (EO)13526, Classified National Security Information, 12-29-2009 (3 Code of Federal Regulations (CFR), 2010 Comp., p. 298-327), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq.), as amended.

TJNAF does, however, possess a limited amount of unclassified information requiring protection, hereafter referred to as Sensitive Information. In August 2022, DOE Order 471.7, Controlled Unclassified Information, was inserted into JSA's contract canceling DOE O 471.3 Identifying and Protecting Official Use Only Information. Subsequently, SC published a Controlled Unclassified Information Program Plan to implement the order and developed a graded approach through the establishment of a three-tiered model for unclassified protected information. This tiered model includes the following: Federal CUI, Contractor Owned Protected Information and Non-Federal Sponsor Protected Information.

TJNAF does have **the following Sensitive Information** requiring safeguarding:

- Controlled Unclassified Information (CUI)
- Contractor Owned Protected Information
- Non-Federal Sponsor Protected Information

Controlled Unclassified Information (CUI)

CUI recently replaced Official Use Only (OUO) under DOE Order 471.7, Controlled Unclassified Information. Information deemed Federal CUI (CUI hereafter) as sponsored and funded directly by a federal organization are to follow the controls outlined below.

TJNAF has a limited amount of CUI, because the information did not come from, or was not created or possessed by or for, DOE or another executive branch agency or an entity acting for an agency.

1. What is 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 (LRGWP) requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

2. Categories of CUI

The categories of CUI are identified on the CUI Registry:
https://www.archives.gov/cui/registry/category-list

If you are unsure whether information should be categorized as CUI, seek guidance from the Security Office at fso@jlab.org or the Cyber Security Office at helpdesk@jlab.org.

Examples of CUI include:

- Export Controlled Technology
- Patents
- Accident Investigations
- Reports obtained from a DOE database
- Technology that falls in the red area of the S&T Risk Matrix

3. CUI Markings

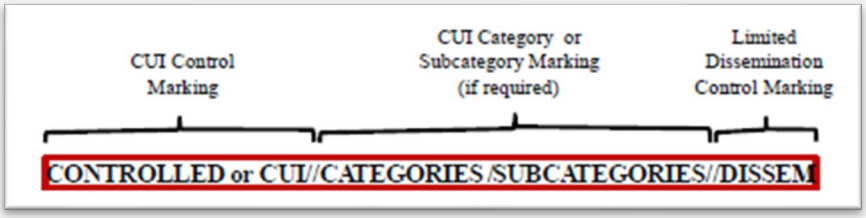
Documents and matter determined to contain CUI must be marked appropriately. The primary marking for all CUI is the CUI Banner Marking. This is the main marking that must appear at the top of each page of any document that contains CUI.

The content of the CUI Banner Marking must be inclusive of all CUI within the document and must be the same on each page. The Banner Marking should be in BOLD capitalized black text and be centered when feasible.

A CUI Banner Marking may include up to three elements:

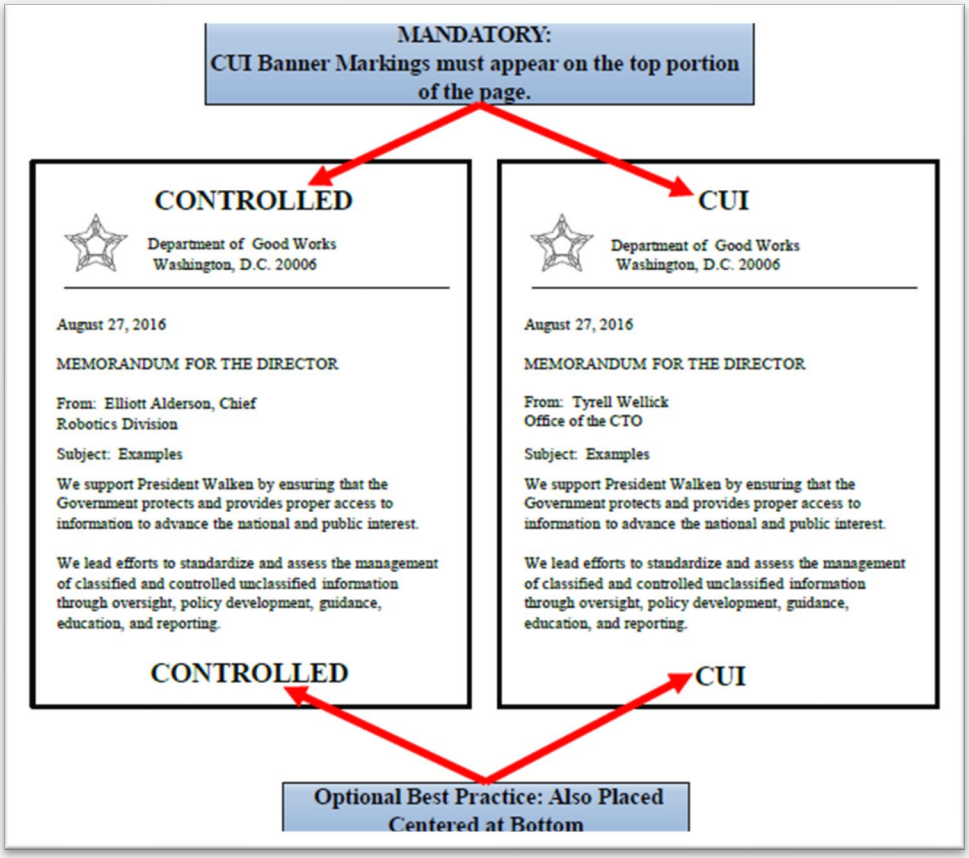
1. The CUI Control Marking (Mandatory) may consist of either the word "CONTROLLED" or the acronym "CUI".
2. CUI Category or Subcategory Markings (mandatory for CUI Specified). These are separated from the CUI Control Marking by a double forward slash (//). When including multiple categories or subcategories in a Banner Marking, they must be alphabetized and are separated by a single forward slash (/).
3. Limited Dissemination Control Markings are preceded by a forward slash (//) to separate them from the rest of the CUI Banner Marking.

Example of a CUI Banner Marking:



NOTE: The above example uses the words "CATEGORIES" and "SUBCATEGORIES" as substitutes for CUI Category or Subcategory Markings and the word "DISSEM" as a substitute for a Limited Dissemination Control Marking. Consult the CUI Registry for actual CUI markings.

At a minimum CUI documents must contain the CUI Control Marking at the top of each page of the document (the placement at the bottom of the document is optional, but is considered a Best Practice):



4. CUI Categories and Subcategories

The CUI program is founded on the prerequisite that only information requiring protection based in a law, Federal regulation, or government-wide policy can qualify as CUI. The CUI Categories and Subcategories are essentially the "flavors" of CUI. Each Category and Subcategory is based in at least one (and sometimes many) of these laws, regulations or government wide policies that require a certain type of information to be protected or restricted in dissemination.

There are two types of CUI Categories and Subcategories:

- CUI Basic and
- CUI Specified

CUI Basic – is, as the name implies, the standard "flavor" of CUI.

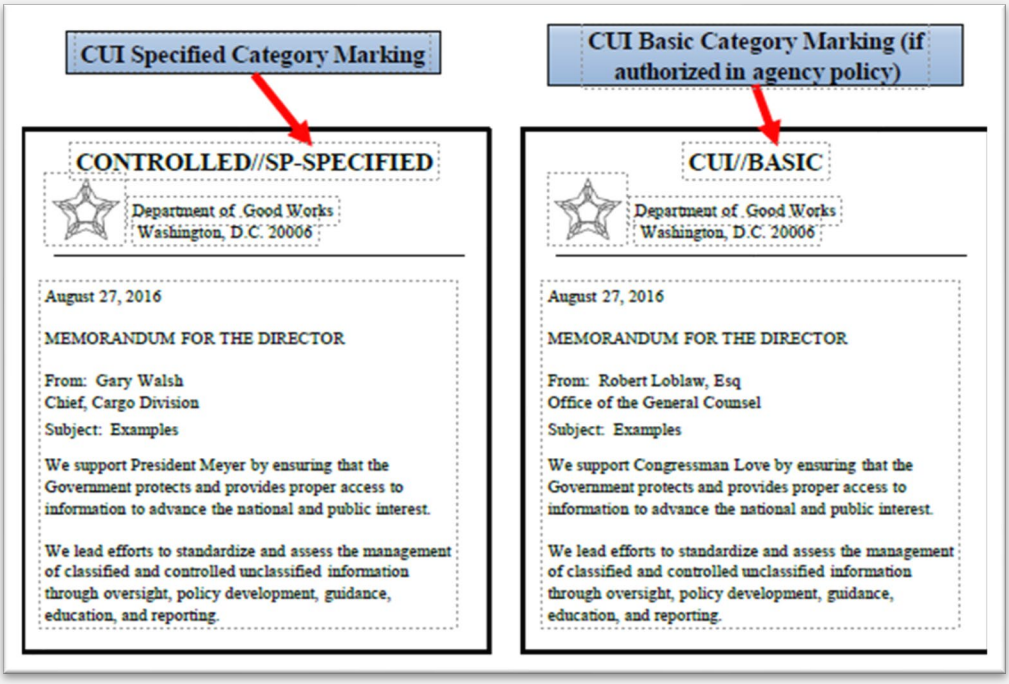
CUI Specified – is different since the requirements for how users must treat each type of information vary with each Category or Subcategory. This is because some Authorities have VERY specific requirements for how to handle the type of information they pertain to – requirements that simply would not 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 laws, Federal regulations, and government-wide policies, they are not things that can legally be ignored or overlooked. As such, a document containing multiple CUI Specified Categories and Subcategories must include ALL of them in the CUI Banner Marking.

There is one additional issue with CUI Specified, in that some CUI Categories and Subcategories are only CUI Specified sometimes.

The reason for this is, as stated above, often there are many different laws or regulations that pertain to the same 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.

Essentially it comes down to this: If the law, regulation, or Government-wide policy that pertains to your agency is listed in the CUI Registry as a Specified Authority, then you must mark the CUI based in that Authority as CUI Specified and include that marking in the CUI Banner. The types are identified under each category or subcategory in the CUI Registry.



NOTE: The above examples use the words "SP-SPECIFIED" and "BASIC" as substitutes for CUI Category and Subcategory Markings. Consult the CUI Registry for actual CUI markings.

5. Marking CUI Specified

Since CUI Specified Categories and Subcategories are different – both from CUI Basic and also from each other – CUI Specified MUST always be included in the CUI Banner.

This is done to ensure that every authorized holder and end user who receives a document containing CUI Specified knows that the document must be treated in a manner that differs from CUI Basic.

We accomplish this marking in two ways:

1. All CUI Specified documents must include the Category or Subcategory marking for all of the CUI Specified contained in that document in the CUI Banner Marking. This ensures that the first thing a user in receipt of that document sees is the CUI Banner letting them know they have something other than just CUI Basic and will have to meet any additional or alternative requirements for the CUI Specified they hold.

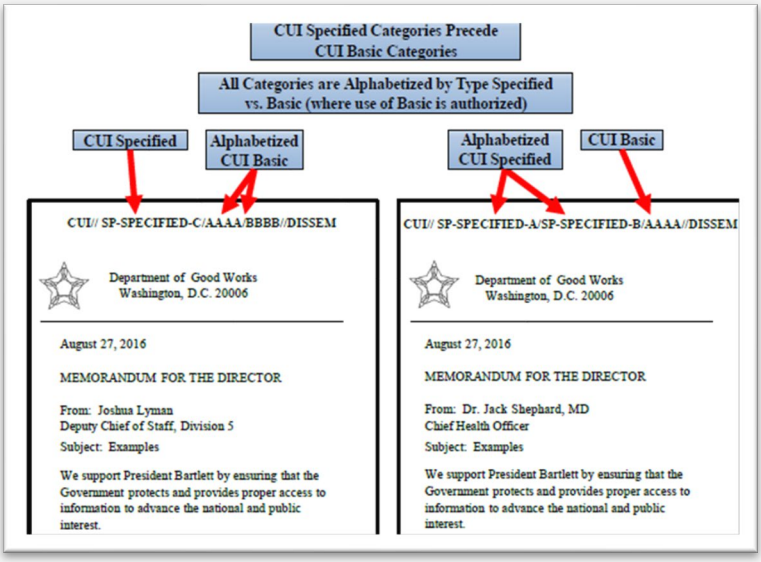
2. To make sure that it is obvious that a Category or Subcategory is Specified, the marking has "SP-" added to the beginning of it.

6. Multiple Category or Subcategory Marking

CUI Specified Markings MUST precede CUI Basic Markings (where authorized for use by the agency head) in the CUI Banner. Consult your agency CUI policy for guidance on use of CUI Basic Category or Subcategory Markings.

CUI Category and Subcategory Markings MUST be alphabetized within CUI type (Basic or Specified).

Alphabetized Specified CUI categories and subcategories MUST precede alphabetized Basic CUI categories and subcategories. Below are examples of CUI Banner Markings used in a document that contains both CUI Specified and CUI Basic:



NOTE: These examples use "AAAA" and "BBBB" as substitutes for CUI Basic Category and Subcategory Markings, "SP-SPECIFIED-X" as a substitute for a CUI Specified Category and Subcategory Markings, and "DISSEM" as a substitute for a Limited Dissemination Control Marking. Consult the CUI Registry for actual CUI markings.

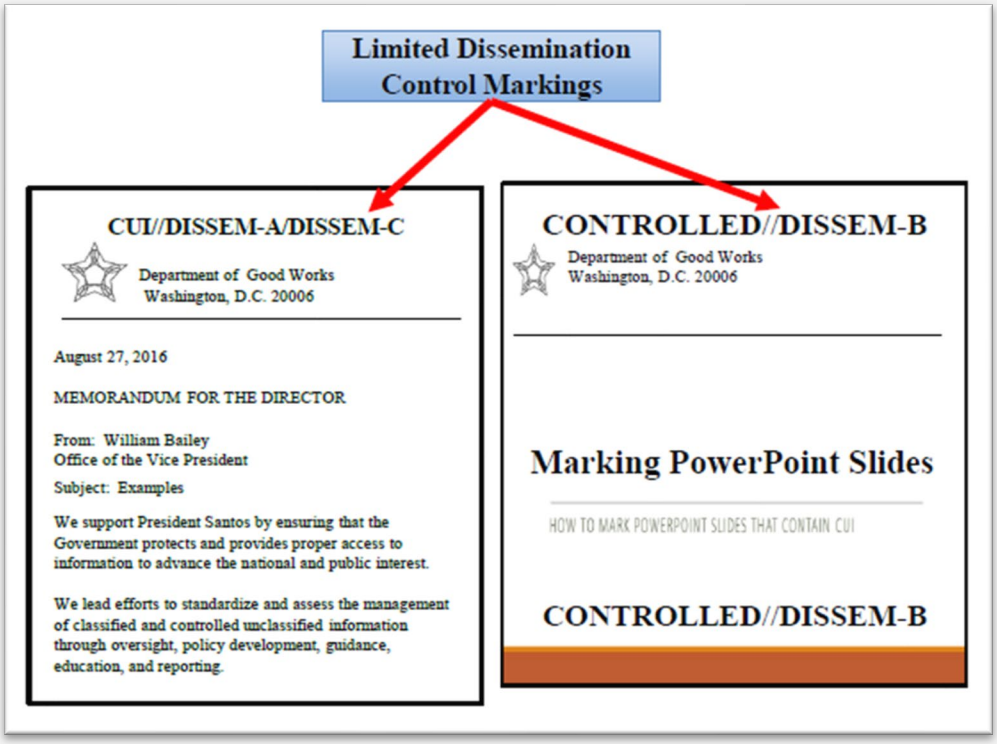
7. Limited Dissemination Controls

Only Limited Dissemination Control Markings found in the CUI Registry are authorized for use with CUI.

Limited Dissemination Control Markings are separated from preceding sections of the CUI Banner Marking by a double forward slash (//).

When a document contains multiple Limited Dissemination Control Markings, those Limited Dissemination Control Markings MUST be alphabetized and separated from each other with a single forward slash (/).

Below are examples that show the proper use of Limited Dissemination Control Markings in the CUI Banner Marking in a letter-type document and a slide presentation.



NOTE: The above example uses "DISSEM-X" as a substitute for Limited Dissemination Control Markings. Consult the CUI Registry for actual CUI markings.

8. Designation Indicator

All documents containing CUI MUST indicate the designator's agency.

This may be accomplished through the use of letterhead, a signature block with agency, or the use of a "Controlled by" line.

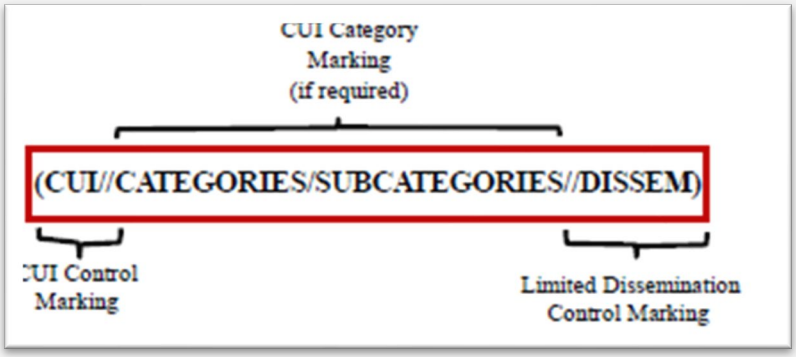
Every effort should be made to identify a point of contact, branch, or division within an organization, and to include contact information.

9. 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. Agency heads may approve the required use of CUI Portion marking on all CUI generated within their agency. As such, users should consult their agency CUI policy when creating CUI documents.

When CUI Portion Marking is used, these rules must be followed:

- CUI Portion Markings are placed at the beginning of the portion to which they apply and must be used throughout the entire document.
- 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 must be the acronym "CUI" (the word "Controlled" will not be used in portion marking).
    2. CUI Category or Subcategory Markings: These can be found in the CUI Registry.
        a. When used, CUI Category or Subcategory Markings are separated from the CUI Control Marking by a double forward slash (//).
        b. When including multiple categories or subcategories in a portion, CUI Category or Subcategory Markings are separated from each other by a single forward slash (/).
    3. Limited Dissemination Control Markings: These can be found in the CUI Registry 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 (/).
- 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 Controlled Unclassified Information.

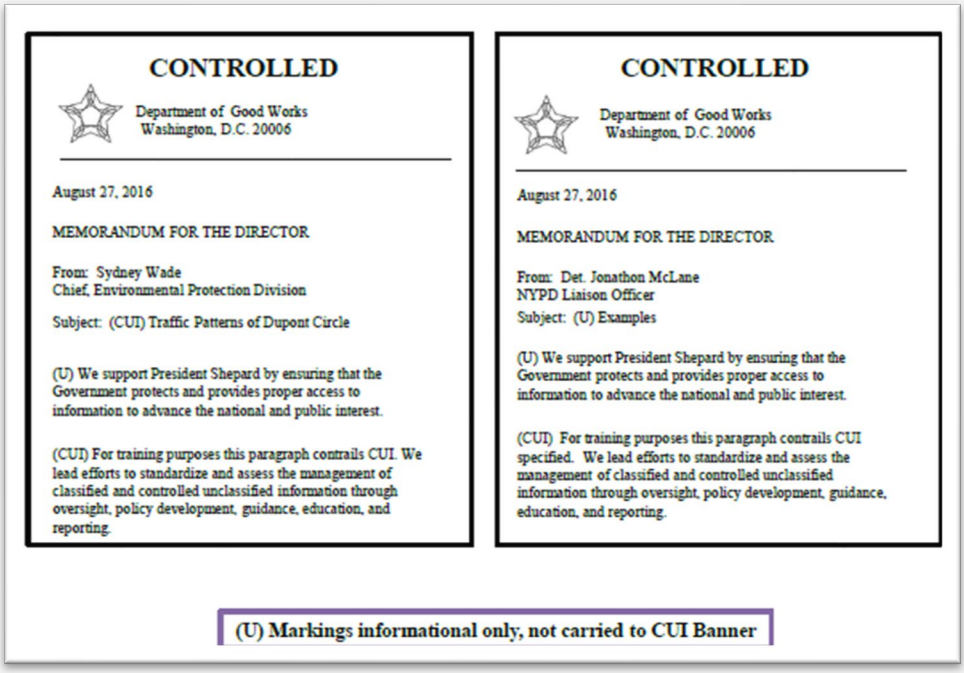


NOTE: The above example uses the words "CATEGORIES" and "SUBCATEGORIES" as substitutes for CUI Category or Subcategory Markings and the word "DISSEM" as a substitute for a Limited Dissemination Control Marking. Consult the CUI Registry for actual CUI markings.

CUI Portion Markings are placed at the beginning of the portion to which they apply and must be used throughout the entire document. They are presented in all capital letters and separated as indicated in this handbook and the CUI Registry.

The presence of EVEN ONE item of CUI in a document requires CUI marking of that document. Because of this, CUI Portion Markings can be of great assistance in determining if a document contains CUI and therefore must be marked as such.

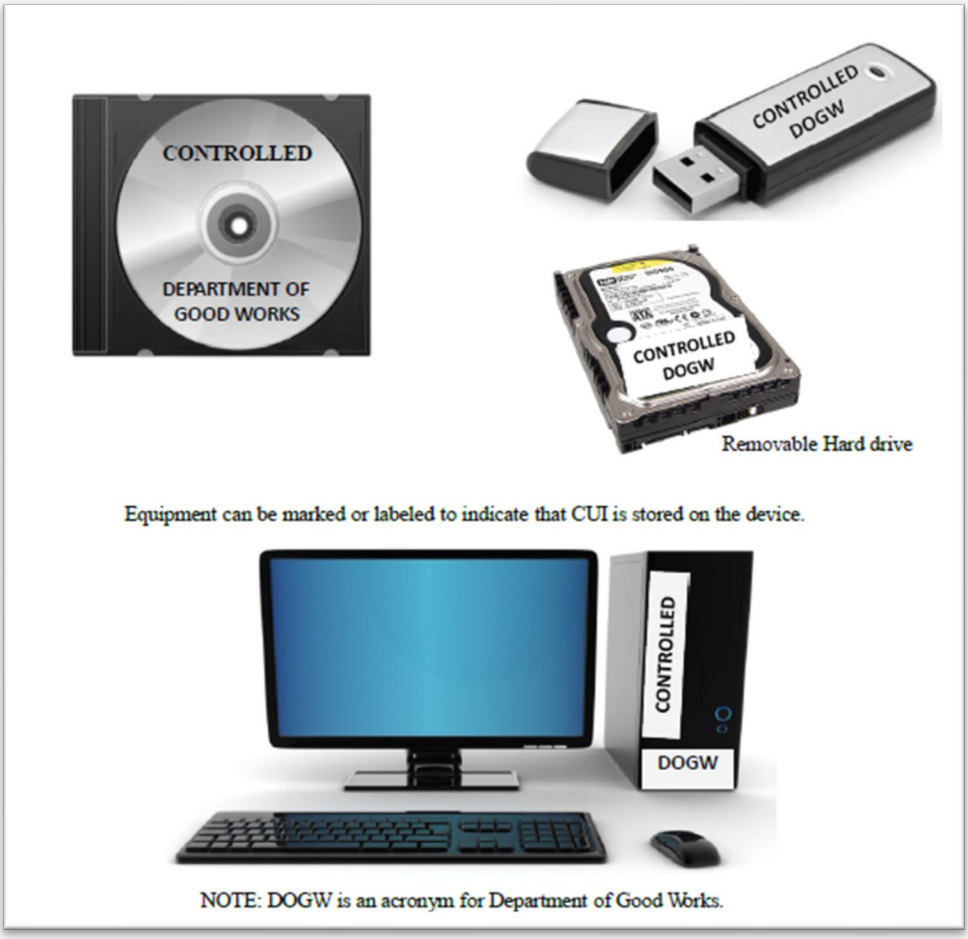
Remember: When portion markings are used and any portion does not contain CUI, a "(U)" is placed in front of that portion to indicate that it contains Uncontrolled - or non-CUI - Unclassified Information.



10. Marking Removable Electronic Media Storing or Processing CUI

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

Due to space limitations it may not be possible to include CUI Category, Subcategory, or Limited Dissemination Control Markings. At a minimum, mark media with the CUI Control Marking ("CONTROLLED" or "CUI") and the designating agency.



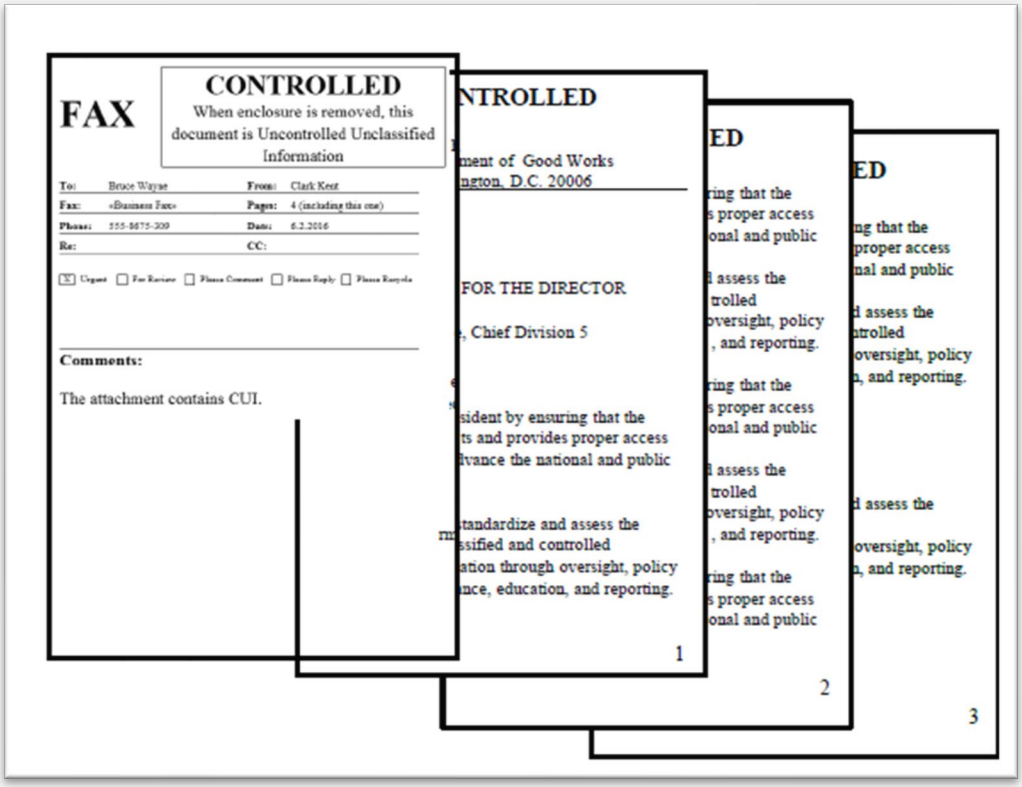
11. Requirements for Sending CUI in Email

- The CUI information must be sent as an attachment
- The attachment itself must be appropriately marked for CUI
- The attachment must be encrypted or protected by a password
- The password must be sent in a separate message or relayed via another means (phone call, etc.)
- The first line in the body of the email must state that the email attachment contains CUI

12. 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, this document is Controlled Unclassified Information; or
    - When enclosure is removed, this document is (CUI Control Level); upon removal, this document does not contain CUI.



13. Container Markings

When an agency is storing CUI, authorized holders should mark the container to indicate that it contains CUI.

Below are some simple applications of this:

14. 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.
- Use in-transit automated tracking and accountability tools where possible.

15. Electronic Storage

When CUI is in an electronic format, the document must contain all of the appropriate markings and may only be stored on approved Jefferson Lab computer systems and cloud services. CUI may not be stored on non-Jefferson Lab computers, tablets, storage media, or mobile devices.

Contractor Owned Protected Information

In addition to CUI, JSA has other forms of sensitive information known as Contractor Owned Protected Information including:

- Business Sensitive
- Personnel Sensitive
- Attorney-Client Privileged

For information to be considered in need of protection, the information must have the potential to damage laboratory, government, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other TJNAF/DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case when confronted with potentially sensitive information. However, information that is available in the public domain is generally not sensitive information.

Business Sensitive

Business sensitive information or data is proprietary and must be protected from unauthorized access, to safeguard the privacy or security of Jefferson Science Associates (JSA)—including anything that poses a risk if discovered by a competitor or the general public. This information/data often has a time limit.

Examples:

1. **Commercial/proprietary** – Trade secrets, business plans, facility floor plans and designs, cost data received from outside the company, personal statements, documents (inspection, reviews, site visits, investigations, audits, etc.) supplied by contractors and received in confidence.
2. **Information Produced by TJNAF** – Basic research, Cooperative Research and Development Agreements (CRADAs), Work for Other Agreements, TJNAF acquisition/evaluation plans, and results of evaluations and audits.
3. **Intellectual Property** – Contract negotiation information, procurement data, patentable design bids, R&D information, and pre-decisional information internal to TJNAF business communications or plans.

Personnel Sensitive

Personnel Sensitive Information is information if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual including personnel and medical files and similar files whose disclosure would constitute a clear unwarranted invasion of privacy. Note, this information usually falls under the protection of the Privacy Act of 1974.

Examples: Employee payroll data, tax reports and payments, payments for employee benefit and welfare plans, travel related costs and information, employee performance information and medical records.

Attorney-Client Privileged Information

Attorney-client privileged information or working papers prepared by an attorney in contemplation of litigation. Contact TJNAF legal counsel for instructions before creating or accepting any information that may be considered "Attorney-Client Privileged Information."

Similar to CUI, other forms of sensitive information must also be marked and stored securely. See the table below for the specifics.

	Marking	Physical Storage	Email / Facsimile Transmission	Hard Copy Transmission
Business Sensitive	• Each page of the document should be marked "Business Sensitive." • Documents marked "Proprietary" are by nature *business sensitive*; no further marking required.	Store in a locked cabinet.	BUSINESS SENSITIVE must be marked in the subject line.	Document must be concealed in an unmarked protective folder and properly controlled at all times.
Personnel Sensitive	Each page of the document should be marked "Personnel Sensitive."	• Store in a locked cabinet. • Must have documented permission from the CISO to store PII on CD, memory stick, etc.	PERSONNEL SENSITIVE must be marked in subject line. When possible to encrypt, protect using approved encryption algorithms (e.g. Entrust). If encryption software is not available, password-protect all attached documents (Microsoft Word and Adobe software) and send the password in a second email. - Information should not be sent in the body of an email message. The Lab's email system is not equipped with an approved encryption software capable of protecting the information.	Hand Carry – Document must be concealed in an unmarked protective folder and properly controlled at all times. Interoffice Mail – Document must be placed in a sealed envelope marked *on the outside* with "Personnel Sensitive – To be opened by recipient only." Mail – Document should be placed in a sealed, opaque envelope on which is written "TO BE OPENED BY ADDRESSEE ONLY." Any commercial carrier can be used but the item must be sent either *first class*, *express*, *certified*, or *registered mail*.
Attorney-Client Privileged	Each page should be marked "Business Sensitive – Attorney Working Papers."	Store in a locked cabinet.	ATTORNEY- CLIENT PRIVILEGED must be marked in subject line.	Document must be concealed in an unmarked protective folder and properly controlled at all times.

If you require assistance to determine whether your documentation/technology is sensitive in nature or you require assistance to determine the type of sensitive information you are in possession of, seek guidance from the Security Office at fso@jlab.org or the Cyber Security Office at helpdesk@jlab.org. When a determination is made, **you are responsible for safeguarding all sensitive information** according to this training.

Non-Federal Sponsor Protected Information

Jefferson Lab has a very limited number of Strategic Partnership Projects with educational institutions and private companies where technology transfer or other business agreements are in place and managed by the Procurement Division. The information sharing and protection requirements outlined in the contract and statement of work should be followed.

Safeguarding Information

JSA employees are responsible for the safekeeping of sensitive information under their control. In addition to the markings and transmission protections the following additional precautions should be taken to protect CUI and all other sensitive information against release to unauthorized persons:

1. **Electronic Storage**
   When in an electronic format, the document must contain all of the appropriate markings and may only be stored on approved Jefferson Lab computer systems (e.g. J and M drives) and cloud services (e.g. MS SharePoint). Sensitive information may not be stored on non-Lab computers, tablets, storage media, or mobile devices. MS SharePoint is recommended for use for securely sharing sensitive information to avoid

2. **While in Use**
   Reasonable precautions should be taken to prevent access to sensitive information by persons who do not require the information to perform their duties. For example, one must not read a CUI document in a public place (e.g., cafeteria or on public transportation). Also, one must not read, discuss, or leave sensitive information unattended where unauthorized personnel are present.

3. **Email**
   When sending CUI and Personnel Sensitive - Contractor Owned Protected Information via email the sensitive information must be in an attachment and protected by encryption or password protection. The password must be transmitted separately from the email attachment containing the sensitive information (e.g. by email, phone or text). Contractor Owned Protected Information including Business Sensitive and Attorney Client Privileged information shall follow the same protection process as above when transmitting information to external recipients not using a Jefferson Lab email address. All other categories of sensitive information may be sent internally without encryption or password protection.

   If reasonable to do so to avoid frequent email transmissions, MS SharePoint is recommended for securely sharing sensitive information with known persons having a Lawful Government Purpose (LGP) who require access to the information to perform their job or other DOE-authorized activities.

4. **Computer Lockout**
   If an employee's computer contains sensitive information, it should either be turned off or have a screen saver that locks out access whenever the employee is away from their desk. Certain applications run by specific groups may have additional security requirements, including secondary passwords or other security features beyond those provided by the central systems.

5. **File Permissions**
   File and directory permissions must be configured to prevent "World Read" and, in most cases, "Group Read" of sensitive information. The Help Desk (helpdesk@lab.org) can assist with setting file and directory permissions.

6. **Locked Offices**
   Offices containing sensitive information must be locked when vacated at the end of each workday.

7. **Networked Printers**
   Extra caution should be exercised when printing sensitive documents using networked printers. An inadvertent compromise of protected information may occur if a document does not print immediately but might be retained in the print queue memory—then printing out at a later date and time when not expected. Malfunctions must be cleared and all paper paths checked for paper containing sensitive information. Excess paper containing sensitive information must be destroyed according to section 4.

8. **Reproduction**
   Documents containing sensitive information may be reproduced to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as the originals.

Retention & Destruction

Due to varied types of CUI and Sensitive information, any questions regarding the retention schedule or destruction should be addressed to the Records and Sensitive Technology Information Manager.

Misuses

All violations of sensitive information due to misuse should be reported to the Facility Security Officer (fso@jlab.org) as soon as the misuse becomes known. Examples of misuse include:

- CUI from a document and matter marked as containing CUI is intentionally released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE-authorized activities.
- A document and matter marked as containing CUI is intentionally or negligently released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE-authorized activities.
- A document and matter that is known to contain CUI is intentionally not marked.
- A document and matter that is known to not contain CUI is intentionally marked as containing such information.

I acknowledge that I have read the policies and procedures and understand my responsibilities as it relates to protecting Sensitive Information.

Click here to receive
completion credit