Controlled Unclassified Information (CUI) Frequently Asked Questions

Are My Research Data / Objects Considered 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. CUI **does not** include classified information. Classified information is explicitly designated as Confidential, Secret, or Top Secret and requires protection for national security reasons.

Examples of CUI include:

- Personally Identifiable Information (PII)
- Proprietary business information
- Export control information
- Law enforcement sensitive data

To determine if your research data or physical objects may be considered CUI, the following steps may be of use:

- **Identify the Source of Research Funding or Regulation**
  - The federal sponsor or regulation is the determiner of whether your research project data or objects may include CUI. ***ASU does not determine if project data or objects are designated as CUI***
  - Examine the source of your project's funding or the governing regulations.
  - CUI is associated with federal research projects or contracts.
  - If your work is federally-funded or involves government agencies (e.g., DoD), there's a possibility CUI may be involved.

- **Review Your Terms**
  - If you are proposing for or receiving a new federal grant or contract, the funding announcement or award terms and conditions may state (e.g. via a CUI clause) that the project could or will involve CUI, and/or you may generate CUI during project performance.

NOTE fundamental research projects **cannot** involve CUI. Before proposing for or accepting grants or contracts with CUI requirements, the project scope should be reviewed to confirm fundamental research (FR) is being performed and if so, proposal applications should explicitly state FR is being performed. Likewise, grant or contract terms should be negotiated to state FR activity is being performed and CUI requirements are thus not applicable. For questions about fundamental research contact export.control@asu.edu. Contact your Proposal or Contracts GCO regarding addressing CUI terms in proposals and awards.

- If the funding announcement for your research proposal application requires you to submit a CUI Control Plan, CUI data may be in scope for the award. Contact your Proposal GCO for assistance with confirming (see bullet above) that the proposed work **isn't** fundamental research. If the work is assessed by ASU to **not** be fundamental research, contact KE Information Security to assist with developing a CUI plan for the application along with providing costs for the CUI system for the proposal budget.
- If your sponsor informs you, after award **and after agreement that CUI is not involved in the project,** that CUI is now applicable, contact the Contracts GCO to renegotiate the award terms and conditions for this new requirement. Contact KE Information Security to assist with developing a CUI plan for the requirement along with providing costs for the CUI system which would be submitted to the sponsor for acceptance.
- Review the terms and conditions of any nondisclosure agreements (NDAs) or Data Use/Protection Agreements (DUAs), especially with federal parties, as these may also include CUI requirements. Contact the Contracts GCO to negotiate these terms and conditions if required, and KE Information Security if systems to control CUI are needed.
- Do not assume that deidentified data for human subjects research is not CUI; confirm with your sponsor and/or contact ASU.IRB@asu.edu.

- **Check Other Communications from your Funding Source (e.g., email)**
  - If your research is funded by DoD, or another government agency or sub-contractor, CUI data may have been identified.

- **Consult the CUI Registry**
  - The CUI Registry lists all categories and subcategories of CUI, along with definitions.

- **Apply CUI Determination Standards**

    - CUI classification is based on federal regulations and standards, such as 32 CFR Part 2002, which defines CUI and mandates safeguarding data related to federal interests.

- **Check with the Office of Research and Sponsored Programs Administration (ORSPA) Proposal and/or Contracts Grants Officers, KE Information Security, or Export Control**
    - These groups can help clarify whether your work involves CUI and can advise you on necessary security protocols.
    - If you have received information that is marked as CUI (whether you agree with the marking or not), please contact ORSPA, export.control@asu.edu, and/or KE Information Security for guidance.

What is not considered CUI?

- Information that is already in the public domain
- Information that is produced through a fundamental research project which is intended for unrestricted publication and broad dissemination
- Information generated from research not funded by the federal government
    - Note: Such information may still be considered confidential or proprietary. Review terms and conditions to determine any special handling requirements.

What is Physical CUI?

While CUI is often associated with electronic data (e.g., digital documents, emails, etc.), it also encompasses a broad range of physical information and objects. CUI may appear in printed documents, notes, records, drawings, blueprints, and even on physical prototypes or models. For example, a research lab might handle printed technical data subject to export control, sensitive project documentation, or personally identifiable information (PII) of study participants—all of which might require the same protection as digital CUI.

Moreover, physical objects like storage media and physical access tools (e.g., keys and badges) that control entry to secure CUI storage areas may also be considered CUI.

By recognizing that CUI extends beyond purely digital formats, KE Information Security can help you and ASU take a more comprehensive approach to securing sensitive information in both the physical and digital domains.

What are some methods to secure Physical CUI?

Methods for protecting physical CUI may include, but are not limited to:

- **Controlled Access:** Implement badge-based systems or biometrics for access to secure areas. Use locked storage, such as safes or file cabinets, to prevent unauthorized access or loss.
- **Physical Barriers:** Secure rooms with reinforced doors, restricted entry points, and monitored access controls. Cover windows to reduce visibility from the outside.
- **Surveillance:** Install cameras, motion sensors, and alarms to deter unauthorized entry. Review footage regularly.
- **Clear Desk Policy:** Require personnel to secure all physical CUI when unattended, ensuring it is not left out in open areas.
- **Destruction:** When no longer needed, use cross-cut shredders or other approved destruction procedures for disposing of physical CUI to prevent recovery.
- **Escort:** Accompany visitors, maintenance, and custodial staff in areas where physical CUI is stored or processed.
- **Logging:** Maintain access logs for CUI storage areas and review regularly.
- **Training and Awareness:** Educate staff on the importance of physical security and their role in protecting CUI.

Table 1: Types of Physical CUI

Printed Research Data	Hard copies of research findings or datasets from federally funded projects may fall under Controlled Technical Information (CTI), a category of CUI established by the NARA.
Grant and Contract Documents	Physical grant proposals and contract documents associated with federal funding may contain sensitive information requiring protection as CUI. Per 32 CFR Part 2002, any information that supports federal missions or national interests must be safeguarded as CUI when it meets specific criteria.
Medical and Healthcare Records	Physical health records used in federally-funded research may also be classified as CUI due to their sensitive nature. Healthcare records from studies involving active-duty military personnel or veterans, such as research funded by

	the Department of Veterans Affairs (VA) or the Department of Defense (DoD).
Export-Controlled Information	Hard copies of schematics, design plans, or technical data related to federal projects subject to the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) when restricted for national security purposes.
Personnel and Student Information	Physical records with personal details of students or personnel involved in federally-funded research, especially when linked to security interests.
Engineering and Technical Blueprints	Hard copies of technical designs or blueprints, particularly those related to defense or critical infrastructure projects funded by federal grants.
Proprietary or Sensitive Project Notes	Researchers' handwritten notes or printed materials containing sensitive project details associated with government contracts are considered Controlled Technical Information (CTI).
Incident Response and Security Plans	Physical copies of incident response or security assessment documents pertaining to the protection of CUI.
Physical Prototypes and Models	Prototypes, physical models, or mock-ups developed under federally-funded research (e.g., defense-related technologies or sensitive materials) if they contain controlled technical or scientific information.
Data Storage Media	Hard drives, USB drives, CDs, DVDs, or other media that contain sensitive data from federal research or CUI.
Laboratory Equipment with Stored Configurations or Results	Specialized equipment like computers, oscilloscopes, or other digital instruments used in research that store configuration settings, test results, or calibration data from federally-funded research if they retain sensitive data.

Physical Research Instruments with Proprietary Technology	Equipment embedded with or based on proprietary technology developed under federal research agreements. This could include experimental machinery, specialized tools, or unique custom-built devices.
Communication Devices with Stored Sensitive Data	Phones, radios, or other communication devices that store data related to sensitive research activities or interactions with federal agencies if they contain stored communications, notes, or other protected information.
Researcher Lab Notebooks and Journals	Physical notebooks or journals used by researchers to record sensitive observations, experimental results, or methodologies, particularly in projects involving controlled scientific information.
Packaging or Shipping Containers with CUI Labels	Physical packaging or containers, used to transport controlled research materials, which are marked with CUI labels.
Physical Keys and Badges	Keys or badges that allow the bearer access to CUI facilities.

What do I do if I receive CUI via physical mail (a CUI marked document) or via email and I did not expect it, or a sponsor says they want to send me CUI?

If you receive physical information marked CUI via regular mail or delivery service, physically secure the information (e.g. locked desk drawer), do not disseminate further and contact KE Information Security for assistance.

For CUI sent via email for which a pre-arranged secure means of electronic receipt is not in place, do not download the CUI onto the ASU network or disseminate further, and contact KE Information Security for assistance.

If a sponsor says they want to send you CUI via email, ask for the “type” of CUI they want to send (e.g. export controlled information) and to hold on emailing it to you in order to confirm a secure means to receive it. Contact KE Information Security for assistance.

How can CUI be involved in a sponsored research award?

For sponsored research, CUI can be 1) provided by the government for proposal application purposes, 2) provided by the government during project performance, or 3) generated by ASU, as determined by the government, during project performance under the sponsored award.

Regarding dedicated systems for proposal assistance, would it be advisable for schools or departments that submit proposals to DARPA or DoD to have dedicated computers that meet the necessary requirements (electronic barrier, NIST SP 800-171, or DoDI 8582.01) to support faculty in proposal preparation and submission?

Contact KE Information Security to discuss on a case-by-case basis. Remember generally speaking, ASU proposal applications should not contain CUI, or be marked CUI, and they should be able to go into the ERA system.

Can I as a Research Administrator (or other personnel) view CUI?

Generally yes. Information marked CUI does not mean it cannot be viewed by Research Administrators or others assisting with proposal application or award administration. CUI can be viewed as long as it is done in a manner that aligns with the controls prescribed for the type of information. If ASU has a system of controls for the CUI in place, and you have a need to know the information (e.g. for proposal and award administration reasons) contact your PI to coordinate viewing the information.

Are Funding Announcements (FOAs) CUI?

No, generally FOAs are public documents and should not be marked as CUI or contain CUI. If a funding announcement is marked CUI, the sponsor should be contacted to confirm whether the funding announcement is indeed CUI, and the marked information should not be disseminated or downloaded onto the ASU network until confirmation is received. If the FOA is confirmed as CUI or specific Government CUI is needed (separately) to respond to a FOA, contact KE Information Security for assistance to securely receive/control/access the information.

What needs to be considered when budgeting CUI requirements?

It is ultimately the responsibility of the PI to fully consider CUI requirements when estimating a budget, Research Administrators and Proposal GCOs can also assist. Some areas to consider may include, but are not limited to:

- **Physical Security:**
    - Secured spaces, including access control
    - Safes or locked cabinets
    - Surveillance/alarm systems
- **IT Support and Security:**
    - Secure networks
    - Encryption tools
    - Endpoint protection
- **Compliance:**
    - Access monitoring, Data Loss Prevention (DLP), and audit logging.
    - CUI labeling/tracking software.
    - Investments in building physical and/or logical environments compliant with the DoD-mandated Cybersecurity Maturity Model Certification (CMMC) certification (which fulfills controls from NIST 800-171).
    - Costs for third-party audits to ensure compliance with CMMC.
    - Certification fees if Compliance mandates formal accreditation.
- **Personnel:**
    - Additional staffing for large proposals (e.g., Information Security Officer, Compliance Analysts, IT Support Staff).
    - Consulting fees for compliance experts and auditors.
- **Training:**
    - Costs involved in training staff on proper CUI handling, incident reporting, and applicable security policies.
- **Policy Development:**
    - There is a significant personnel, cost, and time investment involved in developing a comprehensive, dynamic System Security Plan (SSP), which is a requirement of CMMC.
- **Maintenance:**
    - Physical repairs/alterations
    - Computer/software updates
    - Vulnerability assessment and remediation

Whom do I contact for CUI-Related Proposal Applications?

When a Principal Investigator (PI) is applying for a program that may involve CUI during performance, who do we contact for assistance?

- Contact your Proposal GCO if the FOA includes terms and conditions related to CUI so those terms can be addressed during the proposal application preparation process.

NOTE: CUI cannot be involved in fundamental research projects. Dissemination and access controls on research project information impacts academic freedom, thus a decision to submit an application (and subsequently accept an award) for a research project involving CUI should be considered carefully at the application stage. For questions about fundamental research contact export.control@asu.edu.

- Contact KE Research Technology Office at KE Information Security:
  - To securely receive/control CUI if the FOA indicates that **access** to Government CUI is required to submit a proposal application, and/or there may be a portion of the proposal application that will contain Government CUI.
  - For assistance with budgeting the cost of CUI controls (systems) for the proposal application if it is determined that the project performance will involve CUI. **See FAQ above entitled "What needs to be considered when budgeting CUI requirements?"**

What if the CUI is only accessible through a secure computer system (which the Research Administration team cannot access or review), what is the process for submitting the proposal? Specifically, see the below guidelines state "do not process DARPA CUI on publicly available computers" which presents a challenge, as it limits our ability to access and review the solicitation, thereby impacting our ability to effectively handle these proposal submissions.

Controlled Unclassified Information (CUI) on Non-DoD Information Systems

In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. This information is referred to collectively as Controlled Unclassified Information (CUI). DoD CUI is based on law, regulation, or government-wide policy. DoD CUI Categories are located at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx. For further information, consult DoDI 5200.48, "Controlled Unclassified Information."

All non-DoD entities doing business with DARPA are expected to adhere to the following procedural safeguards, in addition to any other relevant federa or DoD specific procedures, for submission of any proposals to DARPA and any potential business with DARPA:

- Do not process DARPA CUI on publicly available computers or post DARPA CUI to publicly available webpages or websites that have access limited only by domain or Internet protocol restriction.
- Ensure that all DARPA CUI is protected by a physical or electronic barrier when not under direct individual control of an authorized user and limit the transfer or DARPA CUI to subcontractors or teaming partners with a need to know and commitment to this level of protection.
- Ensure that all DARPA CUI is only processed on information technology systems meeting NIST SP 800-171 or DoDI 8582.01 requirements.
- Ensure that DARPA CUI on mobile computing devices is identified and encrypted and all communications on mobile devices or through wireless connections are protected and encrypted.
- All wireless telephone transmission of CUI will be avoided when there are other options available.
- Sanitize or destroy media containing CUI before disposal or release for reuse in accordance with NIST SP 800-88.

Proposers with questions regarding CUI should contact the DARPA Security and Intelligence Directorate at (703) 526-1581.

CUI should not be viewed or processed on systems without the required controls in place. That said, information marked CUI does not mean it cannot be viewed by Research Administrators or others assisting with proposal application and submission. CUI can be accessed and viewed as long as it is conducted in a manner that aligns with its prescribed controls. If a system of controls for the CUI has been put in place contact your PI to coordinate accessing and viewing the information.

What is the Proposal Submission Process when FOAs indicate the project may involve CUI during performance?

If, after review of the proposed project scope and FOA, the proposed scope is assessed by ASU to **not** be fundamental research, contact KE Information Security to assist with developing a CUI plan for the application along with providing costs for the CUI system for the proposal budget.

Even if Government CUI was furnished to assist with proposal development, and ASU has included the expenses for a CUI system in the budget, ASU's proposal application **should not** be marked CUI or contain CUI and it can be saved in ERA.

In rare cases where Government CUI was furnished to assist with proposal development and that CUI must be re-stated in the application for technical reasons, the CUI portion of the proposal should be separated from the non-CUI proposal, marked "CUI-" (per sponsor markings), stored electronically as coordinated with KE Information Security, not go in ERA, and submitted per instructions from the sponsor. Alternative means to manage these situations can be determined case by case and could depend on specific sponsor requirements.

You mentioned that ASU proposals should not include CUI. This is not a problem for internal processes; however, it is likely that technical descriptions in proposals and the final submission documents will contain CUI (to be responsive to the FOA), which cannot be shared or saved via public computers. In this case, who within ASU will be responsible for reviewing and authorizing the submission of proposals if all our computers are considered public? Will PI's be expected to have secure CUI compliant computers to submit the CUI proposals directly instead of the GCO?

A copy of the redacted proposal package, with CUI removed, should be saved in ERA. The Proposal Grant Contract Officer (GCO) need only review the Project Summary/SOW, Budget, and Budget Justification in order to approve for PI submission to sponsor.

In rare cases where Government CUI was furnished to assist with proposal development and that CUI must be re-stated in the application for technical reasons, the CUI portion of the proposal should be separated from the non-CUI proposal, marked "CUI-" (per sponsor markings), stored with government furnished CUI as coordinated with KE Information Security and not go in ERA, and submitted per instructions from the sponsor. KE Information Security may be able to advise on best practice to submit CUI marked proposal documents on a case-by-case basis.

Again, Research Administrators and others should be able to view the CUI marked proposal information as long as it is conducted in a manner that aligns with its prescribed controls for the information. Contact your PI to coordinate accessing and viewing the information.

What happens if the award (in response to an ASU application) states CUI will be involved in project performance?

- Contact KE Information Security for implementation of CUI contract specific requirements (system security plan, etc.) if already budgeted for in the application.
- Contact Contract GCO to review and negotiate the award terms and conditions prior to ASU accepting contracts/agreements, especially if the involvement of CUI was not originally proposed and budgeted for.
- Contact KE Research Compliance at export.control@asu.edu for assistance with general questions or consults related to CUI, export controlled CUI questions, and accessing CUI training, etc.