Controlled Unclassified Information (CUI) Procedures

What is CUI?

Controlled Unclassified Information (CUI) is designated information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies. Information is deemed CUI by the federal government because it is sensitive in nature. There are two CUI registries – the CUI Registry is maintained by the National Archives, and the DOD CUI Registry is maintained by the US Department of Defense (DOD). The improper safeguarding of DOD CUI (also referred to as Covered Defense Information) may impact national security. DOD CUI is unclassified but requires controls to prevent release of information that, if publicly associated with defense missions or aggregated with other sources of information, can reveal exploitable information to US adversaries.

CUI Markings

All CUI must be identified appropriately. CUI markings alert recipients that special handling may be required to comply with law, regulation, or government-wide policy. At a minimum, CUI Basic must be identified by including “CUI” or “CONTROLLED” in the banner and footer (top and bottom) of each page. If CUI Specified, the marking must include the specific authority such as “CUI/SP-CTI”. CUI received from the federal government also usually includes a cover page to clearly identify the document contains CUI.

Each digital file must include the word “CUI” in the naming.

Safeguarding Measures

CUI must be safeguarded to prevent unauthorized access:

- A Technology Control Plan (TCP) is required to be established and maintained at UD for the life of a CUI program. Please contact RO-Agreements with any questions regarding TCPs.
- CUI in printed form must be stored in a controlled environment with physical barriers such as in a locked cabinet marked “CUI” in a limited-access room. A controlled environment is a space or area with adequate physical or procedural controls to limit unauthorized access to CUI.
- CUI must be controlled in compliance with the requirements of NIST SP 800-171.
- CUI may not be transmitted via normal email or UD Dropbox. DOD’s Secure Dropbox system meets CUI requirements for file sharing.
- CUI may be sent using United State Postal Service or overnight mail (e.g., Fedex) if it is only marked as CUI on the inside of the envelope/package and sent to an individual who is approved to receive the CUI.

Trainings

Training courses are offered at no cost to UD faculty, staff, and students:

- The DoD Mandatory Controlled Unclassified Information (CUI) Training fulfills the CUI training requirement when required by the terms of a federal contract.
- All project personnel listed on Technology Control Plans at the University of Delaware are required to complete the “Introduction to Export Compliance” training module on CITI Program prior to beginning work on the project, to be renewed every three years.
- The “Research Security Training (Combined)” course on CITI Program aligns with the training requirements of the CHIPS and Science Act of 2022.

Alternative Work Sites

When necessary, users may utilize “alternate work sites”, defined as government facilities or the user’s private residence. In alignment with on-campus access, users are required to utilize a UD-issued computer to access the VDI, which requires the use of UD’s user authentication software prior to accessing the system. Users must engage in the same physical security of their computers as on campus, such as ensuring the computer screen cannot be seen by unauthorized persons, and that the computer is secured at all times while at the alternate work site to prevent unauthorized access.

CUI Destruction

Printed CUI must be destroyed to a degree that makes the information unreadable, indecipherable, and irrecoverable; no one should be able to identify a letter or a number once the CUI is destroyed. All instances of digital CUI files must be permanently deleted.

Reporting

Actual or suspected mishandling of CUI must be reported, as well as any suspicious behaviors that could potentially compromise or lead to the compromise of CUI. Events involving CUI should immediately be reported to Clarissa Roth, Director of Research Security at clarissa@udel.edu or 302-831-8626.

CUI events include but are not limited to:

- Improper storage of CUI
- Actual or suspected mishandling of CUI
- Unauthorized person gaining access to CUI
- Unauthorized release of CUI (to public facing websites or to unauthorized individuals)
- Suspicious behavior, which may include:
  - General disregard for security procedures.
  - Seeking access to computer systems containing CUI outside the scope of current responsibilities or authorization per the project’s Technology Control Plan.
  - Attempting entrance to locations where CUI is stored, processed, or discussed.

Questions?

Review the project’s Technology Control Plan and contact the Research & Regulatory Affairs department at the Research Office at RO-Agreements@udel.edu.