THE UNIVERSITY OF TEXAS AT EL PASO

MEMORANDUM

To: All Research Investigators

From: Dr. Ahmad M. Itani, Vice President for Research

From: Luis E. Hernandez, Vice President for Information Resources

CC: John S. Weibe, Vice President for Academic Affairs & Provost

CC: College Deans

Subject: Controlled Unclassified Information (CUI) and Budgetary Considerations

Date: October 17, 2025

Controlled Unclassified Information (CUI) is unclassified information the United States Government creates (includes certain funded research) or possesses that requires safeguarding or dissemination controls limiting its distribution to those with a lawful government purpose. CUI may not be released to the public. For the Department of Defense (DoD), CUI also requires controls to safeguard information for national security purposes, such as physical and operations security. The University and all its employees are required to comply with the laws and regulations regarding CUI.

While most research at the University of Texas at El Paso does not involve CUI, it is everybody's responsibility to safeguard the information. If you plan to work with or apply for federal funding that involves CUI, you must consider budget and timeliness implications. The University is providing two (2) significantly cost reducing environments to safely work with CUI. The first option is utilization of the CUI Enclave which is a specialized, purpose-built secure computing environment that processes, transmits, and stores sensitive data. Its primary purpose is to prevent unauthorized disclosure of CUI. The second option is to utilize the Advanced Manufacturing and Aerospace Center (AMAC) facility. The facility is configured with a compliant network security framework and in a manner that meets regulatory requirements for CUI. Although both options meet Federal requirements, Principal Investigators are still responsible for budgeting for hardware (laptops, etc.), specialized software, and other ancillary items\services. We highly encourage you to utilize one of these options for any CUI work that you may conduct.

Vice President for Research & Innovation
500 West University Avenue
El Paso, Texas 79968-0587
915.747.5680
Fax 915.747.6474

If you choose not to utilize either option noted above, you will need to budget for the development of a secure network, hardware, software, and ancillary items\services. You will also be responsible for the development of a System Security Plan (SSP), which must be approved by the Research Security Officer and the Chief Information Security Officer. An SSP is a significant, time-consuming endeavor that can become costly to implement, and is an essential element for compliance with cybersecurity standards like NIST SP 800-171 and frameworks such as the DoD Cybersecurity Maturity Model Certification (CMMC). These requirements must be in place before accepting and beginning any work that involves CUI or requires adherence to CMMC. Depending on the complexity of the project, budgets can exceed $100,000 to ensure you meet CUI regulatory requirements. The University will not fund these costs.

An SSP describes how an information system meets security requirements. When the information system stores, processes, or transmits CUI, the SSP must document how 110 security controls are implemented to safeguard the system, as outlined in NIST SP 800-171. The SSP scope includes the system's hardware, software, and personnel. The SSP is the foundational roadmap for defining the system boundaries (including hardware, software, and personnel), developing incident response plans and implementation of mitigation strategies.

The University of Texas at El Paso is committed to compliance with CUI regulations and the ensuing U.S. export controls. Research & Innovation's Office of Sponsored Projects and Research Compliance and Regulatory Assurances is staffed to advise and assist faculty with CUI identification and budgetary development. More information regarding CUI identification and budget considerations for research projects can be obtained by contacting the Research Security Officer at rso@utep.edu. Information Resources' Information Security Office (ISO) is staffed to advise on network, equipment, and software requirements in addition to providing information on the development of an SSP. They can be reached at security@utep.edu.

Enclosure:
1. Safeguarding CUI Awards Process Flow Chart

Vice President for Research & Innovation
500 West University Avenue
El Paso, Texas 79968-0587
915.747.5680
Fax 915.747.6474

Safeguarding CUI Awards

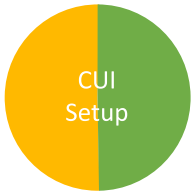
1. Principal Investigator, Research Administrator, Research Security Officer and ISO
If CUI identified at this step, operational and budget requirements (including CUI hardware/software/consulting costs) reviewed and approved.

2. Office of Sponsored Projects
Awards granted from Federal agency flagged and forwarded for CUI review.

3. Research Security Officer
In collaboration with PI, OSP, and award sponsor.
Duration: 5 business days

4. Chief Information Security Officer
<u>Simple Review</u>
Duration: ~2.5 weeks
Ex: Standard Windows 11 laptops/desktops in one campus location
<u>Complex Review</u>
Duration: 2.5+ weeks
Ex: Non-standard systems (e.g., embedded devices, non-Windows OS) across multiple locations

5. Principal Investigator
Collaborates with ISO to safeguard CUI environment (PI leads collaboration effort).
Duration: Dependent on PI's responsiveness, CUI environment complexity, and ISO workload.



6. Research Security Officer
Conducts follow-up with PI to ensure all requirements for CUI plan have been implemented and met.

7. ISO Auditing, and Research Protections, and PI
Auditing and monitoring throughout project execution in collaboration with PI to ensure compliance with the ISO approved protection plan. PI leads safeguarding effort for duration and closeout of award.

October 2025