The National Academies of
SCIENCES · ENGINEERING · MEDICINE

The National Academies
Office of Program Security, Controlled Unclassified Information (CUI) Program

The Controlled Unclassified Information (CUI) Program: Quick Reference Guide

Below are a few key questions everyone should be able to answer about The CUI Program at the National Academy of Sciences.

WHAT IS CONTROLLED UNCLASSIFIED INFORMATION (CUI)?

Controlled Unclassified Information or "CUI" is a term used to describe information that requires protection in accordance with a law, regulation, or government-wide policy. A CUI Program is required by the U.S. government for all Contractors to establish institutional-wide, government-compliant procedures for handling and safeguarding controlled unclassified information.

CUI must be safeguarded to prevent unauthorized access. We protect CUI because failure to do so:

- **Violates a law, regulation, or government-wide policy that call for its protection.**
- **Can have serious adverse effects on governmental and private organizations, organizational operations, assets, or possibly the individuals working within those organizations.**
- **Can cause significant financial loss to the government, private organizations and businesses, and the American people.**
- **Can have direct negative impact on the national security of the United States.**

Most information that may be considered CUI is identified in what is referred to as the "CUI Registry." The CUI Registry is a listing of all categories and subcategories of CUI developed and maintained by the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA). It can include but is not limited to information related to:

- **Critical Infrastructure**
- **Defense**
- **Export Controlled**
- **Financial**
- **Immigration**
- **Intelligence**
- **International Agreements**
- **Law Enforcement**
- **Legal**
- **Natural and Cultural Resources**
- **North Atlantic Treaty Organization (NATO)**
- **Nuclear**
- **Patent**
- **Privacy**
- **Procurement and Acquisition**
- **Proprietary Business Information**
- **Provisional**
- **Statistical**
- **Tax**
- **Transportation**

Here at the Academies, we have established a CUI Program that includes a CUI policy with clear procedures for how we will protect information provided to us from various sources. The NAS CUI Program meets the requirements for government contractors as set forth in Executive Order 13556, 32 CFR Part 2002, and NIST 800-171. Our CUI Program Manager is Enita Williams and the program is staffed by the Office of Program Security.

WHAT DOES THE CUI PROGRAM MEAN FOR **YOU** HERE AT THE NATIONAL ACADEMIES?

Under the program, we each have a responsibility to protect CUI information we have access to. Failing to protect CUI could result in harm to the information owner, impacted parties, and even the inability to do future government work.

YOU must protect CUI by maintaining physical controls, electronic controls, dissemination controls, and destruction/decontrolling requirements. We must:

1. **Safeguard and properly store CUI at all times to ensure the accountability of the information is maintained throughout the life-cycle project and that no unauthorized access to the information occurs. This includes applying CUI Program meeting procedures to limit access to CUI materials and discussions.**
2. **Ensure that all CUI is received (physically and electronically) through channels as established by CUI policy or pre-approved by the CUI Program Manager. CUI *MAY NOT BE TRANSMITTED OVER UNAPPROVED EMAIL SYSTEMS (e.g. @nas.edu, @gmail.com, etc.)* and may not be retained by NAS personnel in hardcopy, or other media format without prior authorization on the CUI Program Manager.**
3. **CUI in electronic format, and well as material derived from access to CUI information, must be accessed and processed on the appropriate NAS Citrix platform.**
4. **Finally, CUI must be properly destroyed or returned to the information owner at the conclusion of the contract. The CUI program handles all necessary CUI destruction and transmission.**

(Continued on Back)

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

The National Academies
Office of Program Security, Controlled Unclassified Information (CUI) Program

NAS CUI Program At-A-Glance

General CUI Program Requirements	NAS CUI Program Policy
Authorized Users	
Access to CUI information must be limited to individuals that have a need to access the information in order to perform his or her contractual duties (i.e. has legitimate "need-to-know"). There should never be a situation or an instance where unauthorized individuals are given access to CUI materials.	For each activity (i.e. board, consensus study, workshop, expert meeting, etc.) an "Authorized User List" must be on file with the CUI Program Manager. The Authorized User list should include all committee, staff, consultants, and participants authorized to access project related CUI. Updates and changes to this list (changing in staff or committee membership) must be provided immediately and in writing to the CUI Program Manager.
Physical Enviornment	
The institution must take reasonable precautions to guard against unauthorized disclosure of CUI in physical environments. This includes: • Controlled environments (where CUI is accessed) • Tracking CUI (inventory all CUI received) • Checking/verifying markings • Storing CUI materials (locked cabinets/marked) • Meetings (procedures to ensure only authorized users are present during times when CUI is accessed.	All CUI must be received, inventoried, processed through the Office of Program Security (OSEC). (Where applicable, CUI materials must be submitted for exemption from the Public Access File.) OSEC, in coordination with the Office of the General Counsel, will verify the control markings are correct and FACA Section 15 requirements are satisfied. In most cases, hard copies of CUI will be authorized for storage with the Responsible Staff Officer (RSO) in a locked cabinet. Where the CUI has heightened safeguarding and handling requirements, the materials must be stored with OSEC.
Electronic Enviornment	
In the electronic environment, CUI transmitted, processed, and stored on institutional systems and networks must be compartmentalized and protected according to an individual's lawful purpose (need-to-know) for access to that information. An institution must have electronic measures in place to ensure unauthorized individuals are prevented from accessing CUI materials. Electronic transmission of CUI is restricted to information technology systems with the proper encryption and security protocols to protect CUI information.	CUI is not permitted on the NAS Enterprise computer system. That means: • **CUI shall not be emailed to or from the Academies' Enterprise email system. Contact OSEC for instructions for CUI electronic transmission.** • **Removable storage devices, such as CDs, USB sticks, and other USB drives (external hard drives) are not authorized for handling and safeguarding CUI materials.** • **Personal devices (e.g. cell phones) and computers should not be used to access CUI related to NAS projects and activities.** Electronic access and processing of CUI must use the Academies' CITRIX platform. Some types of CUI with heightened safeguarding requirements must use the CITRIX/IRM platform (e.g., information already covered by the existing Technology Control Plan). The CITRIX/IRM platforms are administered and managed by the CUI Program Manager.
Destroying and Decontrolling CUI	
CUI must be properly handled and safeguarded throughout the project/contract life cycle. At the conclusion of a project/contract, CUI must be inventoried and either 1.) destroyed by approved destruction method or 2.) returned to the information owner.	At the conclusion of a project/contract activity, the RSO must return all CUI materials in his or her custody to the CUI Program Manager for inventory and destruction/return to the information owner.

FOR QUESTIONS OR ASSISTANCE CONTACT: *Ms. Enita Williams,* Controlled Unclassified Information (CUI) Program Manager, ewilliams@nas.edu, (202) 334-3292 or the Office of Program Security, OSEC@nas.edu, (202) 334-2106.