CUI – Frequently Asked Questions (FAQs)

What is Controlled Unclassified Information (CUI)?

Executive Order 13556 "Controlled Unclassified Information," (the Order), issued on November 4, 2010, established the CUI program, which standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The National Archives and Records Administration (NARA) serves as the Executive Agent to implement this order and oversee agency actions to ensure compliance.

What is the National Institute of Standards and Technology (NIST)?

NIST 800-171 Rev. 2: The National Institute of Standards and Technology **Special Publication 800-171** provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) when resident in Non-Federal Information Systems and Organizations. ***There are over one hundred security requirements in the NIST; this document is summary in nature and not an exhaustive list. See the NIST for complete details***.

What is the DFARS 252.201-7012: Safeguarding Covered Defense Information and Cyber Incident clause?

The clause requires the university to implement security measures as outlined in the **NIST 800-171 Rev 2**. In the event of a cybersecurity incident, the university's responsibility under **DFARS 252.204-7012** is to report the incident to the DoD within 72 hours. The university should preserve and protect images of all known affected information systems identified in this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report.

What is the DFARS 252.204-7000 clause?

Disclosure of Information restricts the release of information unless it is already in the public domain, the Prime Contracting Officer has provided prior written approval, or the results generated during the performance of the project involve no covered defense information and have been determined by the Prime Contracting Officer to constitute fundamental research.

IDENTIFYING CUI

How do we identify CUI?

The University of Arizona's Export Control team works closely with the Contracting Office to identify contracts with NIST requirements or clauses with publication restrictions **(e.g., DFARS 252.204-7012 and 252.204-7000 and others)**. Export Control is also alerted when there are similar safeguards/restriction clauses in contracts that are not sponsored by Department of Defense (some NASA contracts have a similar clause).

An export control checklist is used in the evaluation process. The three-part checklist must be completed by the PI, Contracting Office, and Export Control. The checklist highlights DFARs clauses in addition to potential export control red flags.

What if the 252-204.7000 and/or the 252.204.7012 are in the contract but we think our work is fundamental research?

If both the 7000 and 7012 clauses are included in an agreement, we can contact the Prime Contracting Officer to determine whether the University of Arizona's Scope of Work qualifies as fundamental research. If we receive written confirmation from the prime contracting officer that the university's work is fundamental research, the CUI 7012 clause would not apply. If the project is not considered fundamental research, we would then ask the Prime Contracting Officer to identify which portion of the University of Arizona's research data is considered CUI.

What happens if a project is CUI?

Once a project is determined to involve CUI, it is managed under a security plan. The University of Arizona Export Control Office worked closely with the IT-CUI team to develop "the Plan," a joint Technology Control Plan and System Security Plan. This plan outlines the security measures that researchers and staff must follow to protect CUI data.

ADDRESSING SCENARIOS

Primary CUI Contract Clauses	Requirements	Fundamental Research	Actions
DFARS 252.204-7012 and DFARS 252.204-7000	Safeguarding covered defense information and cyber incident reporting AND disclosure of information (publication restrictions).	NO	**CUI-**Protect according to **NIST 800-171**
		YES	**Written confirmation received from PRIME Contracting Officer-** clauses nullified. **No confirmation**- treat as CUI
DFARS 252.204-7012	Safeguarding covered defense information and cyber incident reporting.	NO	**CUI-** Protect according to **NIST 800-171**
		YES	If contract specifies fundamental/written confirmation from PRIME- clause may be nullified.
DFARS 252.204-7000	Disclosure of Information (Publication restrictions)	NO	Follow restrictions, **not CUI**
		YES	**Written confirmation received from PRIME Contracting Officer-** clauses nullified. **No confirmation**- follow restrictions, **not CUI**
Variety, often from NASA/DHS	Requires an IT Security Plan	YES/NO	Provide information about general IT Security measures.

How might a project be CUI and not export controlled?

A federal sponsor may determine that a project not subject to the EAR or ITAR is nevertheless sensitive and requires additional protection. This may include work in fields outside the applied sciences (such as linguistics, social sciences, or anthropology), research involving sensitive locations (e.g., military installations or government facilities), and/or projects involving cybersecurity or emerging technologies.

RECOMMENDED PARTIES TO INVOLVE

- Contracting (Sponsor and University)
- Information Security/Tech/CIO
- Principal Investigator
- Project personnel
- And of course… Export Control

IT'S CUI- NOW WHAT?

The University of Arizona Export Control office worked closely with the IT-CUI team to develop "The Plan," a joint Technology Control Plan and System Security Plan. This streamlines the onboarding materials and process into one cohesive document, and one joint onboarding briefing.

Protecting and Monitoring CUI

The IT-CUI team (cui-support@list.arizona.edu) oversees access to the CUI environment.

Access Type	Laptop/Desktop	Upload/Download Data	Store Data Locally
"Red Machine"	Currently UA-owned/used	**NO** *Data **only** in AWS /CUI environment*	**NO**
A "red machine" is a UA-owned/issued computer which allows the individual to log into and work in the CUI environment. No information can be uploaded to or downloaded from the CUI environment. No CUI data can be stored locally on this computer.			
"Green Machine"	UA-UITS hardened and provided	**YES**	**YES**
A "green machine" is a UA-owned laptop provided by UITS which allows the individual to not only work within the environment, but information can be pushed to or pulled from the environment. The "green machine" is hardened to meet the NIST 800-171r2 standards. CUI information can be stored and processed locally.			

NOTE: Remote CUI work must be approved in advance by Export Control and the CUI-IT team. There are additional risks associated with remote work.

RESOURCES

National Archives – What is CUI? (pdf)

Obama White House Archives – Executive Order 13556 Controlled Unclassified Information

NIST CRSC – Protecting CUI Information in Nonfederal Systems and Organization Rev. 2 (Abstract)

NIST SP 800 171r2 Protecting CUI Information in Nonfederal Systems and Organizations

DFARS Subpart 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting

Federal News Network - Classified vs Controlled Unclassified Information-What You Should Know

National Archives - CUI Program Implementation, and Features (pdf)

National Archives - About Controlled Unclassified Information (CUI)

National Archives - CUI History

Federal Register - Controlled Unclassified Information

National Archives - CUI Program Blog

National Archives - CUI Training

University of Arizona IT Service Portal

Export Control
University of Arizona
export@arizona.edu
View the Export Control website

Information Technology University of Arizona (UITS)
cui-support@list.arizona.edu