CUI – Frequently Asked Questions (FAQs)
01.11.2021

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 DFAS 252.201-7012: Safeguarding Covered Defense Information and Cyber Incident clause?

This clause requires the university to implement security measures as outlined in the **NIST 800-171**. 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 the information is already in the public domain, the Prime Contracting Officer has given prior written approval, or the results during the performance of the project involved no covered defense information and has been determined by the Prime Contracting Officer to be 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)**. Export Control is also alerted when there are similar safeguards/restriction clauses in contracts that are not sponsored by Department of Defense (NASA contracts often have similar clauses). 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.

This document is simply a reference tool. The regulations should be reviewed prior to making a determination regarding CUI and the accompanying security requirements.

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

If both the 7000 and 7012 clauses are in an agreement we can go back to the prime contracting officer and ask if the University of Arizona's portion on the work is fundamental in nature. If we receive confirmation in writing from the prime contracting officer that the university's work in fundamental it nullifies the CUI clauses.

What happens if a project is CUI?

Once a project is determined to be 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 researchers and staff must follow in order to protect the CUI data.

How is CUI protected and monitored?

University Information Technology Support (UITS)-CUI at the University of Arizona deploys Amazon GovCloud, which can be accessed by the following devices.

ADDRESSING SCENARIOS

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.

This document is simply a reference tool. The regulations should be reviewed prior to making a determination regarding CUI and the accompanying security requirements.

How might a project be CUI and not export controlled? A federal sponsor may determine that a project which is not subject to EAR or ITAR is sensitive and requires additional protections. This could be work in fields other than "applied sciences" (linguistics, social sciences, anthropology), require research and study of sensitive locations (such as military installations or government facilities), and/or involves cyber security or emerging technology.

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.

MONITORING CUI

University Information Technology Support (UITS)-CUI at the University of Arizona deploys Amazon GovCloud, which can be accessed by the following devices.

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 & 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.			

This document is simply a reference tool. The regulations should be reviewed prior to making a determination regarding CUI and the accompanying security requirements.

REMOTE CUI WORK

It is important to point out that we did not wait for requests to work from home to come to us - in March we reached out to PIs and asked how the work from home requirements were impacting their work and if they needed to work from home with CUI data. We implemented a Remote Work Addendum which outlines key risks associated with working from home and risk mitigation requirements.

Risks that we identified include:

1. Unknown levels of physical and cyber security in off campus locations.
2. Unknown visitors with potential access to documents/items/laptops.
3. Inability for UA to assess levels of security directly or to provide oversight.
4. Increases likelihood of work from other locations outside of the home (e.g., coffee shops).
5. Potentially reduces awareness of a possible breach.
6. Greater potential for access by unauthorized individuals.
7. No option to connect to specialized instruments or equipment.
8. Physical support needs for green machines will be extremely difficult.

Required mitigations include:

1. Work must only occur at the location(s) indicated, with notifications of any additional locations.
2. Acknowledgement that working off-campus is only permitted due to extraordinary circumstances and that work will resume on campus when UA has given notice that normal operations can resume.
3. Report any suspicious activity/theft as soon as possible.
4. Use only University issued computers (no personal devices), up to date on patches, and running malware / anti-virus software.
5. Application of security measures identified in the TCP such as:
    - Locking screens when leaving computers with a strong password.
    - Not permitting other people in the room while reviewing data or conducting research.
    - Not taking equipment, data, or documents to any public spaces.

RESOURCES

https://www.archives.gov/files/cui/documents/cui-overview-powerpoint.pdf

https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

https://federalnewsradio.com/records-management-month/2016/11/classified-vs-controlled-unclassified-information-know/

https://www.nist.gov/system/files/documents/2018/10/18/cui18oct2018-0930-1030-cui_overview-casey.pdf

https://www.archives.gov/cui/about

https://www.archives.gov/cui/cui-history

https://www.archives.gov/cui/chronology.html

https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

https://www.archives.gov/cui/additional-tools

https://isoo.blogs.archives.gov/

https://www.archives.gov/cui/training.html

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

https://it.arizona.edu/sites/default/files/documentation/CUI-CDI-NIST-800-171-Onboarding_0.pdf

UA Export Control Program (UECP)
University of Arizona
export@arizona.edu
View our website at https://rgw.arizona.edu/compliance/export-control-program

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

This document is simply a reference tool. The regulations should be reviewed prior to making a determination regarding CUI and the accompanying security requirements.