FCI and CUI Laws, Regulations, and Government-wide Policy

Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) **require safeguarding or dissemination controls** pursuant to and consistent with applicable law, regulations, and government-wide policy.

Keywords: Fundamental Research, Federal Contract Information (FCI), Controlled Unclassified Information (CUI), Cybersecurity Maturity Model Certification (CMMC), Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulations Supplement (DFARS)

Fundamental Research

"Fundamental research means basic and applied research in science and engineering, the results of which **ordinarily are published and shared broadly** within the scientific community, as distinguished from proprietary research and from Industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reason." [National Security Decision Directive (NSDD) 189, National Policy on the Transfer of Scientific, Technical, and Engineering Information].

Federal Contract Information

Federal contract information (from 48 CFR 52.204-21) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. Non-federal systems that store, process, or transmit FCI must follow, at a minimum, the basic safeguarding requirements outlined in FAR clause 52.204-21.

Controlled Unclassified Information

Established by Executive Order 13556 (The Order), the Controlled Unclassified Information (CUI) program standardizes the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, Federal regulations, and Government-wide policies. CUI replaces legacy marking like FOUO (For Official Use Only) and SBU (Sensitive but Unclassified).

In order to qualify for federal contracts that require safeguarding of CUI, the University must implement a compliant infrastructure. NIST Special Publication 800-171 specifies the security requirements for protecting CUI in non-federal systems. In addition to compliance with NIST 800-171, each federal agency has specific policies for safeguarding Controlled Unclassified Information. For example, Department of Defense requirements are specified within DFARS 252.204 clauses. In order to continue doing business with the DoD, all contractors will need to be certified by a Cybersecurity Maturity Model Certification (CMMC) Third-Party Assessment Organization (C3PAO) when the CMMC final rule is published, anticipated to be in late 2024 or early 2025.

CUI Categories

The Order specifies categories of non-classified information to be safeguarded and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the CUI program. NARA maintains official CUI categories and subcategories. For a full listing, please visit CUI Registry General Guidelines site. The DoD version of the CUI Categories can be found at https://www.dodcui.mil/.

CUI Specified and CUI Basic

CUI Specified is the subset of CUI for which there are specific handling controls. When working with *CUI Specified* there are additional specific requirements that must be met as specified by the federal agency or as specified by authorizing law, regulation, or Government- wide policy.

CUI Basic is the subset of CUI that does not have specific handling or dissemination control.

When working on a proposal submission or on a new award, it is important to determine whether CUI protection is required. Look for the following (or similar) clauses to determine if CUI is involved. If so, notify your research security officer at rso@utep.edu for guidance on how to comply with Federal regulations.

FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
Federal contract information (FCI) is defined in 48 CFR 52.204-21. FCI is information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Executive Order 13556 (The Order) - Controlled Unclassified Information
The Order establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. NARA maintains the official CUI Registry for the Federal Government: https://www.archives.gov/cui.

32 CFR Part 2002 - Controlled Unclassified Information
Part 2002 establishes designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. This regulation affects Federal executive branch agencies that handle CUI and all organizations that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.

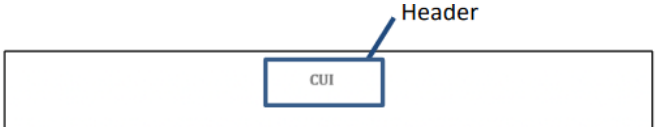
NIST SP 800-171 Rev. 3 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
This publication defines the requirements necessary to protect CUI Basic on non-Federal information systems. To continue receiving Federal funds associated with the use of this data (either directly received from the government or indirectly through associated covered contracts and contractors), UTEP and its research enterprise must ensure all systems and processes involved with CUI are compliant with NIST 800-171.

DoDI Instruction 5200.48 - Controlled Unclassified Information (CUI)
This Instruction establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DOD and establishes the official DOD CUI Registry: https://www.dodcui.mil/CUI-Registry-New/.

DFARS
DFARS is a set of cybersecurity regulations that the Department of Defense imposes on Defense Industrial Base (DIB) contractors, including Higher Education Institutions. One or more DFARS clauses may be included in a Department of Defense-related Request for Proposal (RFP), Request for Information (RFI), or contract**.** An example is DFARS 252.204-7012 which requires that the researcher and University meet NIST 800-171 Rev. 2 standards to protect CUI.

CMMC
The Department of Defense (DoD) has created the Cybersecurity Maturity Model Certification (CMMC) as a way to verify compliance with the CUI security standards of NIST 800-171. This certification will ultimately be required for any entity that seeks to contract with the DoD. DFARS 252.204-7021 specifies CMMC requirements.

The following is an example of a CUI document. If you see the CUI or similar marking in the Header and/or Footer of a document, this means the document is CUI and your system will require controls if stored or processed on the system.



Other keywords to look for that may indicate CUI protections are necessary include: Government Controlled Data, OPSEC, Cybersecurity Questionnaire, etc. It is important to note that each federal agency implements their own CUI program including NASA, DoE, Dept. of Agriculture, and DHS. Thus, it may be necessary to reach out to the agency for guidance on whether a proposal or award is subject to CUI requirements.