Data Classifications at CSU
We currently have three types of data classifications at CSU: **Public, Restricted and Private**. **Public** data is data explicitly made available to the public, such as directory data and published data. **Restricted** data may be used only within the confines of the University, and accessed only by employees of the University needing such access in the conduct of University business. **Private** data is the most sensitive data at CSU, subject to the greatest protections. It can only be accessed with specific authorization, and includes data such as: social security numbers, credit card information, proprietary research information, and personal health information.

Controlled Unclassified Information
**Controlled Unclassified Information** is a federal designation for data that requires certain safeguards and protections. According to the National Archives and Records Administration, which manages the CUI Program, "Federal agencies routinely generate, use, store, and share information that, while not meeting the threshold for classification as national security or atomic energy information, requires some level of protection from unauthorized access and release." The program was established in 2010 by Executive Order 13556; in 2015 the National Institute of Standards and Technology released **SP 800-171** to provide guidance and practices for the protection of CUI. Compliance with SP 800-171 is currently by self-attestation.

Cybersecurity Maturity Model Certification
The **CMMC** is a program currently being implemented by the **Department of Defense** for the protection of CUI, and closely aligns with NIST SP 800-171. However, instead of self-attestation, compliance with the controls and practices in CMMC require third-party certification. According to the CMMC program, "The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain." CMMC involves five levels of cybersecurity maturity, including **Level 1: Basic Cyber Hygiene**, required for all DoD contracts by 2026, and **Level 3: Good Cyber Hygiene**, required for all DoD contracts involving CUI by 2026.

Clauses
- DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (CUI)
- FAR Clause 52.204-21: Basic Safeguarding of Covered Contractor Information Systems (FCI)
- DFARS Clause 252.204-7019: Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS Clause 252.204-7020: NIST SP 800-171 DoD Assessment Requirements
- DFARS Clause 252.204-7021: Cybersecurity Maturity Model Certification Requirement
Reach out to your department IT, Division of IT or Sarah Robinson with the Cybersecurity Services Team (sarah.robinson@colostate.edu) if you have any questions or concerns.