

Management of Controlled Unclassified Information (CUI)

OVERVIEW

In an effort to streamline the management of sensitive information, 32 CFR Part 2002 established a process for management of unclassified information that is to be protected from public disclosure. Any project at University of Colorado Boulder that incorporates the responsibility for managing Controlled Unclassified Information (CUI), must take the appropriate measures to protect the sensitive information.

SCOTT MAIZE (scott.maize@colorado.edu), CU Boulder's Research Cyber Security Program Manager, is empowered to review each program for CUI compliance and work with faculty and staff to ensure that the appropriate steps are taken.



RESEARCH IMPACT

For research activities that incorporate Controlled Unclassified Information (CUI) by reference (or through NIST 800-171r1 or DFARS 252.204-7012), the Office of Information Security (OIS) will need to conduct an additional review, prior to award acceptance.

REVIEW PROCESS

Once OIS is notified of an agreement that may include the requirement to manage CUI, OIS will contact the PI or assigned representative to initiate the cyber security review. They will work in conjunction with the PI or assigned representative to identify and plan to implement the necessary security controls. Once the review has been conducted, OCG will be notified by OIS whether the computing environment that is supporting the project, will be compliant. At that point, they will finalize the review of the contract.

What Steps Do I Take?

Proposal Stage >>

Notify your Office of Contracts and Grants (OCG) Proposal Analyst

Award Stage >>

If you received a notification that the award is subject to CUI, notify your OCG Contract Officer

Any Stage >>

Reach out to Scott Maize for questions about CUI

QUESTIONS?

Contact Scott Maize | scott.maize@colorado.edu