Controlled Unclassified Information Award Lifecycle Procedures

Background:

Controlled Unclassified Information (CUI) is a designation of protected information from the federal government with specific information security requirements. Due to the nature of these regulatory requirements, it is essential for Principal Investigators (PI) to be aware if they are receiving or generating any CUI during the course of a research project and if so to work with their Senior Research Administrator in the Office of Sponsored Programs (OSP), the staff of the Secure and Global Research (SGR) office in the Office of the Vice President for Research (OVPR), and the Cybersecurity and Privacy (C&P) unit in the Division of IT (DoIT), as well as college and department level IT personnel, as early in the research project lifecycle as possible and continuing through the end of the project.

Proposal:

The first step in the CUI Award Lifecycle is the Proposal Stage, in which the PI proposes a new or continued research project. It is not always evident at this stage that CUI will be involved in the project, but if it is known, the Kuali Research Proposal Development proposal should indicate "Yes" to the Questionnaire question "Do you anticipate that this project will involve restrictions such as export controls, controlled unclassified information (CUI), or classified information and/or work?" Additionally, this is the best time to involve SGR and C&P.

Pre-Award:

The second step is pre-award, when the University receives the terms of a contract for a research project, and OSP SRA has an opportunity to negotiate the terms of the contract. The first and best way of addressing CUI requirements is to verify which specific aspects of the data or the project are within the scope of the regulations. This can be identified by DFARS Clauses 252.204-7012/7019/7020/7021, or FAR 52.204-21. Oftentimes it is the case that these clauses are present, but no CUI is expected to be received or generated by CSU during the course of the project, in which case the SRA will attempt to negotiate with the sponsor to add a statement specifying that is the case and that if that changes as the project progresses that the sponsor will provide prior notification to CSU so we can do the necessary preparation to protect the data. If CUI is expected to be part of the project, it is important to identify explicitly in the agreement what data will be considered CUI so the appropriate security mechanisms and processes can be put into place. The most important security mechanism is a System Security Plan (SSP) which describes the technological systems that will be used to generate, use, store, or transfer the CUI. It is the responsibility of the PI to create the SSP, with assistance from SGR, C&P and the relevant college/department IT personnel. <u>The creation of an SSP is not a trivial process and needs to begin as soon as possible</u>. A sponsored project account cannot be created and work on the project cannot begin until the SSP is in place. For certain contracts with the Department of Defense, it may also be required at this time to calculate a compliance score based on the SSP. As per the regulations, every person on the project who will be handling CUI will be required to take CUI training. It is also highly recommended that if a project's contract contains the CUI clauses, even if CUI is not expected to be part of the project conducted at CSU, that the PI and relevant key personnel on the project take the CUI training so they know how to identify, handle and safeguard CUI if it becomes part of the project.

Award Administration:

Once the contract is signed and the SSP is in place if needed, the 53 Account is set up and work on the project begins. During the execution of the sponsored project the terms may change depending on phase or direction

the research leads. If a Phase Change involves a change in CUI scope, the research administrator or the PI will need to alert SGR and C&P and an SSP may need to be created or amended. The project may also be subject to additional review of security terms and practices.

Project Closeout:

Upon project completion, regulated data may need to be sanitized from relevant devices, or archived appropriately in accordance with the contract terms. At this point, the PI and/or research administrator will also need to alert SGR and C&P to ensure data management compliance.