Safeguarding Covered Defense Information, Controlled Unclassified Information (CUI), and Cyber Incident Reporting

Policies

Collected Rules and Regulations, 110.005 Acceptable Use Policy:
https://www.umsystem.edu/ums/rules/collected_rules/facilities/ch110/110.005_acceptable_use_policy

Finance Policies 12000, 12001, 12003:
https://www.umsystem.edu/ums/policies/general_administration

Forms

None

Overview

Effective **December 31, 2017**, in order to accept a contract funded by the US Department of Defense (DoD) or any other agency that contains or is otherwise subject to Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, the University of Missouri must agree to implement the information security standards in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to safeguard systems and networks that process, store, or transmit covered defense information (CDI).

Covered defense information as defined in DFARS 252.204-7012 is Controlled Unclassified Information or controlled technical information.

- Controlled Unclassified Information (CUI) is information the government creates or possesses, or the university creates or possesses on behalf of the government, to which access or distribution controls have been applied in accordance with laws, regulations or Government-wide policies. CUI does not include classified information, nor does it include information the university possesses and maintains in its own systems that did not come from, nor was created or possessed by or for a Government agency. A full list of information types (categories & subcategories) is available at the CUI Registry of the National Archives.
- Controlled technical information has military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information will typically be designated by the use of DoD distribution statements B through F. (DoD distribution statement A identifies technical information that is publicly available without restriction and does not qualify as controlled technical information.)

Covered defense information will be "marked or otherwise identified in the contract, task order, or deliver order" before being provided to, or generated by, the university. In a contract containing DFARS 252.204-7012, this will most often (but not always) be specified in the Contract Data Requirements List (CDRLs), where the sponsor will indicate whether specific data associated with the project is required to be marked as controlled technical information.

DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting

This regulation requires the university to provide adequate security to safeguard covered information that is processed, stored, or transmitted on its internal information systems or networks by using NIST SP 800-171 as the performance-based standard to ensure compliance with the regulation. The university must also flow down this requirement to all subcontractors who will receive or generate CDI through their performance on the contract.

National Institute of Standards & Technology (NIST) Special Publication (SP) 800-171 - Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations

This publication details the mandatory controls for both federal and non-federal agencies, including requirements governing policy, process, and secure IT configuration. The mapping table in Appendix D NIST SP 800-171 maps each requirement to the relevant security controls, and although there are 110 security requirements, these can be grouped into the fourteen categories outlined in the table.

Meeting the NIST Information Technology standard – the University Framework

By directing the university to execute a contract and accept the award, the PI is agreeing to comply and implement the controls. There are multiple components required for compliance with the NIST standards. In this document, the university is defining the framework for institutional compliance and the obligations assumed by a Principal Investigator.

The PI must be able to demonstrate implementation or planned implementation of the security requirements with a system security plan and associated plans of action documentation. PIs can work with their local IT personnel to develop the following:

- **System security plan (Security requirement 3.12.4)** – A System Security Plan (SSP) describes how the University meets the security controls; it is a document that is periodically updated to describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems. Federal agencies may require that a SSP be submitted in a proposal package or prior to award, and may consider the University's system security plan and plans of action as critical inputs to the evaluation factor in the contract selection process. How and if this will be used in the proposal evaluation must be stated in the solicitation. A template can be found on the NIST SP 800-171 website.
- **Plans of Action (Security Requirement 3.12.2)** - A document used to describe individual, isolated, or temporary deficiencies and the management plan designed to correct the deficiencies and reduce or eliminate vulnerabilities in the University's systems utilized by the researcher. A template can be found on the NIST SP 800-171 website.

DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements
DFARS 252.204-7020 – NISP SP 800-171 DoD Assessment Requirements

Recognizing that the process set forth in DFARS 252.204-7012 does not provide a mechanism for the DoD to verify that the NSP SP 800-171 controls have been met and there is the potential that CUI can be stored, processed, or transmitted in a non-compliant environment, additional DFARS clauses (DFARS 252.204-7019 & 252.204-7020) may apply to require that contractors conduct a self-assessment of their NIST SP 800-171 implementation (using NIST methodology) and submit to the DoD prior to award.

Risk

The University's failure to implement NIST SP 800-171 compliant security requirements when contractually obligated to do so could result in the organization's inability to retain existing or receive future affected defense contracts that include the DFARS 252.204-7012 cybersecurity clause.

The Defense Contract Management Agency (DCMA) has audit responsibilities for this contractual requirement. Where it has confirmed that applicable cybersecurity clauses are in the contract, DCMA may audit the university to verify the PI has created a system security plan. If DCMA detects or is made aware of potential cybersecurity issue, DCMA will notify the contractor, DoD program office, and the DoD Chief Information Officer (CIO).

Procedure

The Office of Sponsored Programs Administration (OSPA), the Office of Export Controls (OEC), and the Division of IT (DoIT) will assist PIs as outlined below. The PI should work with his or her department IT professionals to determine what steps to take to ensure compliance with the additional security requirements under a contract containing (DFARS) 252.204-7012 or similar requirements. Departmental IT professionals will engage campus Information Security and Access Management (ISAM) as needed to ensure a smooth and compliant implementation of the requirements. The PI, local IT and ISAM will work together to develop the required System Security Plan (SSP).

In addition to developing a SSP, for contracts subject to DFARS 252.204-7019 or 252.204-7020, the PI—in conjunction with departmental IT and campus ISAM personnel—will conduct a Self-Assessment of the covered information system using the government's methodology. OSPA will verify that summary level scores from that Assessment are posted in the Supplier Performance Risk System (SPRS).

Note that information resulting from or arising during the project that has been determined in writing from the contracting officer to be "fundamental research" is not CUI or controlled technical information and not subject to the security requirements of DFAR 252.204-7012. If a PI believes a project meets the definition of "fundamental research", please contact OSPA and/or the OEC.

Responsibilities

Principal Investigator: The PI must work with his or her department IT professionals to determine what steps to take to ensure compliance with the additional security requirements under a contract containing (DFARS) 252.204-7012 or similar requirements. The PI ensures that no project work begins until all security requirements have been met.

Office of Research OEC: The OEC will work with the PI to identify covered defense information invoking the safeguarding requirement and will assist in determining what safeguards are needed to ensure compliance with the DFARS clause or other regulations. The OEC will also be engaged in implementing the SSP. If needed, the OEC will work with the PI to develop and implement a separate Technology Control Plan (TCP) in accordance with the Standard Operating Procedure for Technology Control Plans. The OEC will communicate the completion of the SSP and TCP to the SGCA.

OSPA
Preaward: At the **proposal stage**, the Pre-Award Senior Grants and Contracts Administrator (SGCA) will identify contracts with this requirement through solicitation review. Once identified the SGCA will inform the PI and the OEC of this clause. If the PI believes his or her research project meets the definition of "fundamental research", the SGCA will work with the PI to ensure an appropriate statement to that effect is included in the proposal documents submitted to the sponsoring agency. If the project does not meet the definition of "fundamental research", the PI will have an opportunity to include the cost necessary to meet the requirements within the proposal budget. According to the DOD Chief Information Officer, the solicitation may require or allow elements of the system security plan, which demonstrate implementation of NIST SP 800-171, or documentation that the results of a Self-Assessment is available in the SPRS, to be included with the proposal. Ultimately, by submitting a proposal with this requirement, the university is representing its compliance.

At the **award stage**, the SGCA will notify the OEC that an award which contains DFAR 252.204-7012 or similar requirements has been received. In cases where the award is for "fundamental research", the OEC will notify the SGCA when the award has been reviewed. In awards where the research project is not for "fundamental research", or the DFARS clause is required, the SGCA will facilitate the work of the PI and the OEC to develop and finalize the required SSP and TCP to meet the contract requirements. By their review and signature of the SSP, the PI is thereby signifying that he or she has implemented all of the NIST 800-171 controls and is aware of his or her responsibilities to protect the CUI and/or controlled technical informaiton. Confirmation of the finalized SSP and TCP is communicated to the SGCA from the OEC. It is at this time that the SGCA will obtain the authorized official's signature on the final sponsor award/contract and issue the final Grant Award Summary (GAS) which includes the MoCode. In all cases, a MoCode is not issued until all compliance assurances have been received by the SGCA.

Related Topics
Identifying and Managing Restricted Research (Export Control)

Creation Date
06/28/2018

Latest Revision Date
12/21/2020

Office of Sponsored Programs
Administration 310 Jesse Hall | Columbia,
MO 65211-1230 573-882-7560 |
grantsdc@missouri.edu

Office of Sponsored Programs Administration
University of Missouri