15.05.03 Secure Computing Enclave Management

Approved February 10, 2020
Next Scheduled Review: February 10, 2025

Regulation Summary

As recipients of federal funding, The Texas A&M University System (system) is required to comply with certain information protection standards commensurate to the level of U.S. government information handled, processed, used, shared, or received. This regulation establishes the framework for management and use of the system's secure computing enclave (SCE).

Regulation

1. RESEARCH SECURITY OFFICE

1.1 The chief research security officer (CRSO) administers the functions of the system Research Security Office (RSO) to include administration, management, and security of the system's SCE, a shared service for use by all members.

1.2 The RSO defines, establishes, and authorizes information security standards and systems to comply with the requirements of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. The RSO maintains the system SCE, an NIST SP 800-171 compliant secure computing enclave.

1.3 The RSO manages onboarding and offboarding processes related to the system SCE, as well as secures access to the system's SCE.

1.4 Member-Proposed SCEs

(a) The RSO serves as the authorizing official for any system SCE and provides attestation of compliance to the U.S. Department of Defense chief information officer.

(b) The RSO must review, assess, and validate all system-established SCEs proposed by member chief information officers (CIOs) for compliance with the NIST SP 800-171 requirements.

(c) The RSO will provide a reference blueprint, standard operating procedures, and technical assistance for members that choose to establish their own SCEs pursuant to this section.

(d) Any enclave established within the system must comply with the specifications established in the reference blueprint, the RSO information security standards, and standard operating procedures.

2. SYSTEM SCE

2.1 Any member may request to utilize the system SCE.

2.2 The RSO developed the *System Secure Computing Enclave Manual* and internal operating procedures governing the administration, management, and security of the system SCE. Supplemental standards include, but are not limited to:

(a) Security Compliance (access control; audit and accountability; awareness and training; configuration management, identification and authorization; incident response; maintenance; media protection; personnel security; physical protection; risk assessment; security assessment controls; system and communications protection controls; and system and information integrity); and

(b) Operations Management (access management; availability management; capacity management; change management; demand management; even management; financial management; incident management; knowledge management; problem management; release and deployment management; request fulfillment; service asset and configuration management; service catalog management; information technology service continuity; service level management; service portfolio management; service reporting and measurement; service validation and testing; supplier management; and transition planning and support).

3. SECURITY OPERATIONS

3.1 Pursuant to System Policy *15.05, Research Security Office*, the RSO will serve as the point of contact for ensuring compliance with all aspects of the U.S. Department of Defense (DoD) Cyber Security Maturity Model (CSMM).

3.2 Accordingly, the RSO will obtain a third party certification determination related to the system SCE as it pertains to the DoD CSMM.

Related Statutes, Policies, or Requirements

System Policy 15.02, *Export Controls Program Management*

System Policy 15.05, *Research Security Office*

System Regulation 15.05.02, *Controlled Unclassified Information Management*

System Secure Computing Enclave Manual (not yet available)

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

System Research Security Office
(979) 862-1965