15.05.01 Classified Information Management

Revised February 16, 2023
Next Scheduled Review: February 16, 2028
Click to view Revision History.

Regulation Summary

As a recipient of U.S. Department of Defense and Department of Energy "facility clearance," The Texas A&M University System (system) is obligated to follow National Industrial Security Program (NISP) requirements, restrictions and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. government executive branch departments and agencies to their contractors.

This regulation establishes guidelines to ensure the system's compliance with guidance provided in 32 CFR Part 117, National Industrial Security Program Operating Manual Rule (NISPOM).

Definitions

Click to view Definitions.

Regulation

1. SECURITY PROCEDURES

1.1 The system has been issued a U.S. Department of Defense and Department of Energy facility clearance to participate in the NISP. Having been granted this facility clearance, the system is subject to the rules and regulations contained in the NISPOM.

1.2 The facility security officer (FSO), appointed by the chancellor, is directly responsible for the receipt, storage, reclassification, declassification, and destruction of classified information. All requests for clearance of employees who require access to classified information at their work location or when visiting other facilities are initiated by the FSO. All authorizations for security clearance are in writing and are not valid until authenticated by the FSO or designee.

1.3 All members may utilize the designated security storage facilities in College Station, Texas, or obtain clearance for additional storage facilities through the FSO.

1.4 The Defense Counterintelligence and Security Agency (DCSA) conducts periodic inspections of system industrial security practices on behalf of the Department of Defense and the Department of Energy. The FSO or designee must conduct self-inspections to ensure continued compliance with the NISPOM. Self-inspections are performed using the most recent *Self-inspection Handbook for NISP Contractors* produced for DCSA by the Center for Development of Security Excellence.

1.5 The FSO must develop detailed Standard Practice Procedures (SPP) to ensure system compliance with the NISPOM. Contact the FSO for questions relating to classified information.

2. INFORMATION SYSTEMS SECURITY

2.1 Classified information must not be processed on information systems that have not been certified and accredited following NISPOM and the Industrial Security Field Operations (ISFO)'s *Process Manual for the Certification and Accreditation of Classified Systems* under the NISPOM.

2.2 The FSO must appoint an information systems security manager and information systems security officer(s) as appropriate.

2.3 The FSO must develop appropriate SPPs to implement the requirements of the NISPOM and the ISFO's *Process Manual*.

2.4 In coordination with members, the FSO must develop classified information cleanup procedures to provide guidance for the removal of classified data from unclassified member networks.

3. DISCLOSURE OF CLASSIFIED INFORMATION

3.1 Individuals authorized to access classified information must follow established procedures at all times, and are responsible for guarding against unauthorized disclosure of classified information.

3.2 Cleared employees must ensure that classified information is disclosed only to persons authorized by NISPOM.

3.3 Employees must not disclose classified or controlled unclassified information about a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification or as specified by the Government Contracting Authority (GCA). Requests for approval must be routed through the FSO to Sponsored Research Services for approval by the GCA.

4. SECURITY VIOLATIONS

4.1 Any violation of established security procedures must be reported to the FSO immediately so the FSO may assist in bringing the situation back into compliance. Examples of security violations are:

(a) Leaving a safe containing classified material open and unattended.

(b) Allowing non-cleared individuals to have access to classified material, either by viewing classified material or by conducting classified discussions in a non-secured area or over a non-secure telephone line.

(c) Allowing non-cleared individuals access to combinations for safes in which classified material is stored.

(d) Sending classified material via fax machines.

(e) Removing classified material from the building in which it is normally stored without permission from the FSO.

(f) Copying or destroying classified material.

(g) Generating classified material on a non-approved computer.

(h) Storing the written combination to a safe in a non-approved container.

Security violations are recorded by the FSO in the Security Incident Report. The FSO must investigate the violation.

4.2 In addition to disciplinary action that may be taken under other system policies, NISPOM requires a graduated scale of disciplinary actions in cases of employee violations or negligence.

(a) **Minor violations** will result in a joint review by the FSO of proper security procedures with the individual. The Security Incident Report is kept in the employee's security file at the system Research Security Office (RSO).

(b) A **second minor violation** results in the employee being required to participate in a complete review of the NISPOM requirements. The Security Incident Report is provided to the employee's university president, agency director, or college dean where the classified work is being performed.

(c) **Additional minor violations** indicate a negligence pattern resulting in an Adverse Information Report submitted to the DCSA. The Security Incident Report and the Adverse Information Report are provided to the employee's university president, agency director or college dean where the classified work is being performed. A decision is made by the university president, agency director, or college dean regarding the appropriate corrective action to be taken which may be up to, and include, denying the individual future access to classified information.

(d) **Major violations include the loss, compromise, and suspected compromise of classified information.** Classified material that is out of the control of its custodian or that cannot be found is presumed to be lost until an investigation determines otherwise. If an investigation determines that classified material is lost, the employee is denied access to classified information for at least one year. The actual length of time for lack of access is determined by the employee's university president, agency director or college dean in which the classified work was being performed and the management group of the system delegated to administer government classified contracts. All major violations are reported to the DCSA Field Office.

4.3 Individual Culpability Reports. When individual responsibility for a security violation can be determined and one or more of the following factors are evident, an Individual Culpability Report is sent to DCSA.

(a) Deliberate disregard of security requirements.

(b) Gross negligence in the handling of classified material.

(c) A pattern of negligence or carelessness.

5. INSIDER THREAT PROCEDURE

5.1 The FSO must create an Insider Threat Program, in accordance with NISPOM.

5.2 The chancellor must designate an insider threat program senior official in writing. This individual may also be the FSO.

5.3 The Insider Threat Program addresses threats to personnel, facilities, material, information, equipment or other Department of Defense, Department of Energy or U.S. government assets. It applies equally to classified, controlled unclassified, or unclassified information related to U.S. government contracts and national security information.

5.4 The FSO must develop standards for the system Insider Threat Program.

5.5 The FSO must work with member compliance officers to establish Insider Threat procedures tailored to each member.

Related Statutes, Policies, or Requirements

Atomic Energy Act of 1954, 42 U.S.C. §§ 2011, *et seq.*

Exec. Order No. 12829, 58 Fed. Reg. 3479 (Jan. 6, 1993).

Exec. Order No. 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995).

32 CFR Part 117 NISPOM Rule

Self-Inspection Handbook for NISP Contractors

System Policy *15.05, System Research Security Office*

Prior to this regulation's February 6, 2020 version, this regulation was published as Regulation *15.99.02, Classified Information*.

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Research Security
(979) 862-1965