15.02 Export Control Program Management

Revised February 9, 2023 (MO -2023)
Next Scheduled Review: February 9, 2028
Click to view Revision History.

Policy Summary

The Texas A&M University System (system) and its members are committed to upholding the highest standard of ethical conduct and compliance with its legal obligations, including federal statutes and regulations implementing U.S. export control policies. This policy establishes the framework for coordinating export control program management activities within and between the members, and establishes mechanisms to ensure that each member develops, implements, and maintains an appropriate export control compliance program.

Policy

1. BACKGROUND

The U.S. government (USG) administers strategically driven statutes and controls certain exports and re-exports for national and economic security. Through the Arms Export Control Act (AECA), the International Emergency Economic Powers Act (IEEPA), the Trading with the Enemy Act (TEA), the Export Control Reform Act of 2018 (ECRA), and other legislation, the USG regulates exports of items, technologies, software, and services to protect U.S. national and economic security. National Security Presidential Memorandum 33 (NSPM-33) was issued to protect U.S.-funded scientific research from foreign interference and exploitation in the U.S.-based research ecosystem, with export control compliance as a foundational component of required research security programs. The purposes of export control-related statutes are to:

(a) Prevent the transfer of sensitive items and technology that could cause harm to the U.S. or its allies' interests.

(b) Achieve a balance in safeguarding sensitive interests and the economic value of exports.

(c) Implement U.S. foreign policy or domestic political concerns.

(d) Implement sanctions as a policy alternative or supplement to either diplomacy or war.

(e) Further multi-lateral agreements in which the U.S. participates.

This policy applies to all faculty, staff, employees, and visiting scholars. Individuals are responsible for the export control implications of their work. Each member will assist faculty, staff, students, and visiting scholars in assessing the applicability of export control statutes and regulations. Definitions of export control statute or regulation terminology, including but not limited to, "export," "defense service," "Empowered Official," "foreign person," "person,"

"technical information," and "U.S. person" are commensurate to those contained in the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), or relative Office of Foreign Assets Control (OFAC) sanction program.

2. SYSTEM RESEARCH SECURITY OFFICE (RSO)

2.1 The system RSO is the responsible office with administrative oversight of member export control compliance programs. For purposes of this policy, administrative oversight is designed to ensure that each member develops, implements, and maintains an appropriate export control compliance program and to facilitate and coordinate export control compliance program management within and between members. The system RSO has unrestricted access to all export control-related operations, records, information, property, and personnel to carry out this policy. The system RSO has the independence necessary to carry out duties effectively without fear of retaliation.

2.2 The system RSO leads the system Export Control Affinity Group (SECAG). SECAG works collectively to develop common results for effective risk-based mitigation within and between members. Common results provide each system member the flexibility to develop procedures that are appropriate for their institution's level of risk. Outcomes (i.e., procedural or methodology changes) of other internal export controls working groups must be reviewed by the system RSO, and those working groups must be inclusive of all affected members.

2.3 The system RSO maintains the system's Directorate of Defense Trade Controls (DDTC) and Bureau of Industry and Security (BIS) Snap-R registrations. Members will not register with DDTC or BIS Snap-R separately. Member legacy DDTC or BIS Snap-R accounts must be administratively moved under the system umbrella.

2.4 As a shared service, the system RSO provides members with export control-specific software resources, including restricted party screening applications.

3. MEMBER RESPONSIBILITIES

3.1 Each member must identify an Empowered Official (EO). According to 22 CFR 120.67, the EO is a member employee who:

(a) Is a U.S. person and is in a position of authority for policy or management.

(b) Is empowered in writing to sign export control-related license applications or other approval requests on behalf of the member.

(c) Understands provisions and requirements of export control statutes and regulations, as well as criminal liability, civil liability, and administrative penalties for export control-related violations.

(d) Has the independent authority to inquire into any proposed export control-related activity by the member, verify the legality of the transaction and accuracy of the information, and refuse to sign any export control-related license application or other requests for approval without prejudice or other adverse recourse.

3.2 Each member must develop a rule implementing an export control compliance program to reduce the risk of potential export control violations. Compliance programs must include the following elements:

(a) Management commitment.

(b) Continuous risk assessment.

(c) Export authorizations, classifications, and jurisdiction requests.

(d) Formal written export control management and compliance program procedures.

(e) Recordkeeping.

(f) Training.

(g) Internal compliance monitoring and periodic audits.

(h) Internal procedures for handling compliance issues, including reporting violations and taking corrective actions.

The compliance program must include procedures to screen potential restricted end-users and end-uses, methods to identify, account for, and protect (where applicable) items and information subject to the EAR or ITAR, procedures for assessing research and services subject to the EAR or ITAR, international travel requests (including an assessment of items and information taken abroad, and enhanced requirements for members subject to NSPM-33), international shipping, visiting scholars, employment, and acquisition of gifts, goods, and services.

3.3 Annually, each member must conduct an export controls-specific risk assessment before starting each fiscal year. The risk assessment includes identifying the member's export control risk portfolio and corresponding risk mitigation strategies. The member risk assessment must be attached to the member's annual ethics and compliance program plan.

3.4 Monthly, each member must share applications and all associated documents regarding visiting scholars and employment of foreign persons from countries of concern as defined in System Regulation *15.05.04, High Risk Global Engagements and High Risk International Collaborations,* to satisfy the requirements of the federal government's insider threat program.

3.5 Each member must provide the system RSO with a courtesy copy of any export control-related license application, license, commodity jurisdiction request (application and determination), commodity classification request (application and determination), documentation of general license use, or advisory opinion.

4. VIOLATIONS

Each member is responsible for reporting known export control violations to the cognizant federal agency as prescribed by law, under the member's established internal reporting requirements, and in consultation with the system RSO and Office of General Counsel (OGC).

Members must report known or suspected violations to the system RSO as soon as possible. The system RSO will promptly notify appropriate system officials, including the vice chancellor for research, OGC, and the system ethics and compliance officer. Members must coordinate all activities associated with voluntary disclosures with the RSO. This includes, but is not limited to, initial voluntary self-disclosure notifications, internal reviews, final voluntary self-disclosure notifications, and coordination with federal regulatory bodies during the disclosure and review process.

Related Statutes, Policies, or Requirements

International Traffic in Arms Regulations (ITAR) 22 CFR 120-130

Export Administration Regulations (EAR) 15 CFR 730-774

Office of Foreign Assets Control (OFAC) 31 CFR 500-598

National Security Decision Directive 189

Atomic Energy Act of 1954 and Nuclear Regulatory Commission Regulations to 10 CFR Part 110

National Security Presidential Memorandum 33 (NSPM-33)

System Policy *15.05, System Research Security Office*

System Regulation *15.05.04, High Risk Global Engagements and High Risk International Collaborations*

System Regulation *16.01.01, Ethics and Compliance Programs*

Member Rule Requirements

A rule is required to supplement this policy. See Section 3.2.

Contact Office

Research Security
(979) 862-1965