CRR Chapter 430:

430.020 Export Control and Sanctions Compliance

Executive Order No. 49, issued 1-24-23; Amended 11-21XX-24

A. Statement of Purpose

1. This rule addresses the University's compliance with U.S. export control and sanctions laws and regulations ("export controls"). The University is committed to export control compliance in all activities that may result in an export or sanctioned transaction with a foreign person, entity, or country.

2. ~~This rule applies to all transactions by the University of Missouri,~~ Unless otherwise indicated, this policy applies to all transactions by the University of Missouri System, its administration, and four universities and all of their component parts (hereafter referred to as "University" or "UM System"), regardless of whether or not those transactions are research related, and is intended to comply with the Foreign Assets Control Regulations ("FACR") at 31 CFR §§ 500-599, the International Traffic in Arms Regulations ("ITAR") at 22 CFR §§ 120-130, the Export Administration Regulations ("EAR") at 15 CFR §§ 730-799, the Foreign Trade Regulations ("FTR") at 15 CFR § 30, and other similar regulations to which export controls or sanctions apply.

B. Scope and Compliance Policy

1. This rule applies to all University employees, students, contractors, consultants, and any other persons acting on behalf of or at the direction of the University.

2. No person may do or facilitate anyone doing any of the following on behalf of the University:

   a. Engaging in transactions prohibited by the Foreign Assets Control Regulations (FACR) or other sanctions programs administered by the U.S. Department of the Treasury, unless otherwise authorized;

   b. Exporting items, technical data, or defense services subject to the ITAR other than as authorized by the U.S. Department of State;

   c. Exporting items, technology, or software subject to the EAR other than as authorized by the U.S. Department of Commerce; or

   d. Violating any other U.S. export control law or regulation.

3. All persons must be mindful of export control requirements across all University activities. This includes, but is not limited to, the considerations listed below. This list is only illustrative, and compliance will be determined by applicable statutes and regulations in place at the relevant time, so all persons should seek guidance whenever activities may involve exports or involve interactions with countries, persons, or entities subject to sanctions.

a. Performing any service of value for a person or entity located in a sanctioned destination (regardless of that person's citizenship) may be regulated by the FACR.

b. The ITAR and EAR regulate the transfer of controlled items, technical data, technology, and software to foreign persons or destinations, in addition to regulating defense services. An export may include:

   1) An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;

   2) Releasing or otherwise transferring technical data or technology (including software) to a foreign person in the United States (a "deemed export");

   3) Transferring registration, control, or ownership of any spacecraft, aircraft, vessel, or satellite by a U.S. Person to a foreign person;

   4) Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;

   5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or

   6) The release of previously encrypted technical data.

c. The following types of technical data, technology, and software generally may be exempt from export control regulations:

   1) Publicly available information. Technical data and technology may be considered publicly available when they are generally accessible or available to the public through sales at newsstands and bookstores; through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; through second class mailing privileges granted by the U.S. Government; at libraries open to the public or from which the public can obtain documents; through patents available at any patent office; through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States; or through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency.

   2) Educational information. Technical data may be considered educational information when it is general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities. Technology may be considered educational information when it is released by instruction in a catalog course or associated teaching laboratory of an academic institution.

   3) Fundamental Research. Fundamental research generally may mean basic and applied research in science and engineering,

the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons. Fundamental research should not be considered to apply to information and software received during the course of research. It should only be considered to apply to the technical data, technology, and software that arises from or is generated during the research. In order for technical data, technology, and software to qualify as fundamental research, the research:

   a. Must be conducted by an accredited institution of higher learning;

   b. Must take place in the U.S.; and

   c. The University and its researchers cannot have accepted other restrictions on publication of or access to scientific and technical information resulting from the project or activity.

C. University of Missouri Research Security and Compliance Team

   1. UM Research Security and Compliance Team

   Each ~~of the four universities within the University of Missouri System is responsible for designating a minimum of one compliance point of contact (POC) related to export compliance~~University within the UM System will have at least one ~~dedicated~~designated export controls and sanctions point of contact (POC) who reports to the UM System Director of Research Security and Compliance. The UM System Director of Research Security and Compliance, research security contacts designated pursuant to CRR 330.120.C.1, and all POCs comprise the University of Missouri Research Security and Compliance Team ("UM RSC Team"). Additional personnel with ~~personnel with~~ compliance responsibilities related to export controls and/or sanctions may be consulted by the UM RSC Team or included within the UM RSC Team at the designation of the UM System Director for Research Security and Compliance.

   2. Collaboration

   Recognizing both the necessity and administrative efficiencies gained, the UM RSC Team shall work in collaboration to meet the needs of the UM System.

   3. Accountability and Alignment

   To ensure the accountability and alignment of the UM RSC Team, each Chancellor shall designate one of that University's Vice Chancellors ~~for Research~~ to work with ~~and~~ the UM System Director for Research Security and Compliance, who will ~~are~~ jointly ~~responsible for approving~~ approve the following as it relates to the POCs and other export controls and/or sanctions professionals at each institution:

      a. Recruitment and hiring decisions
      b. Disciplinary and termination decisions
      c. Annual performance evaluations and compensation decisions.

   For situations in which concurrence is not reached, the collective decision will

be made with the President.

D. Strategies

1. The Director of Research Security and Compliance, in collaboration with the UM RSC Team, will develop the export compliance strategies for the UM System to establish, document, and implement processes needed to ensure that the University, and its personnel, remain in full compliance with applicable U.S. export control and sanctions related laws and regulations while still achieving its academic and global outreach missions.

2. These strategies ~~will be~~ are outlined in an Export Compliance Management Program (ECMP) which operationalizes this policy, establishes processes, reiterates its commitment to compliance, and provides information and guidance to the University community.

3. Each university has the flexibility to develop university specific export compliance and sanctions strategies and procedures after consultation with the Director of Research Security and Compliance and so long as the strategies are not in conflict with or interfere with the UM System export compliance strategies.

E. Implementation

The University of Missouri Research Security and Compliance Team is responsible for the implementation of the export controls and sanctions compliance strategies for the UM System.