EXPORT COMPLIANCE MANUAL

Export Control Officer: Niko Pittore, npittore@ors.msstate.edu, 662-325-8682 **(Main Point of Contact)**
Research Security Officer, Assistant Director: Chris Jenkins, cjenkins@ors.msstate.edu, 662-325-0400

Element 8→ Purpose

The purpose of this manual is to express policies, responsibilities, and processes pertaining to the Mississippi State University (MSU) Export Control Program, which falls under the Research Security section of the Office of Research Compliance & Security (ORC&S). This manual is designed to show that MSU's export program aligns with MSU Export Control Policy 70.04 and government expectations listed in the Bureau of Industry and Security's Export Compliance Guidelines, which can be found here: https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file.

The export of certain commodities, technologies, software, and services outside the United States is regulated by the United States Government (USG) for reasons of national security, foreign policy, the non-proliferation of weapons of mass destruction, counterterrorism, protection of human rights, and for competitive trade. Also regulated under the export control statute is "deemed export", which is the transfer or release of controlled information, technology or software source code that occurs when such controlled data is obtained by foreign nationals within the U.S.

This manual, accompanied by MSU Policy 70.04, is designed to comply with export control laws and regulations. These include but are not limited to ITAR, EAR, and OFAC:

> • International Traffic in Arms Regulations (ITAR), U.S. Department of State, Directorate of Defense Trade Controls (22 C.F.R. 120-130)

> • Export Administration Regulations (EAR), U.S. Department of Commerce, Bureau of Industry & Security (Title 15, Sections 730-774 of the Code of Federal Regulations)

> • Office of Foreign Assets Control (OFAC), U.S. Treasury Department (31 C.F.R. 500-598)

The Export Control Officer (ECO) reports to the Research Security Officer (RSO), who is also the Empowered Official.

Element 1→ Management Commitment
MSU has demonstrated its commitment to export compliance by establishing an overarching policy endorsed by the Office of the President and the Office of General Counsel. MSU also has a dedicated full-time position of Export Control Officer. ORC&S has budgeted and purchased additional screening tools as well as funding travel and training opportunities for the ECO to utilize.

Element 2→ Risk Assessment
How does MSU mitigate export compliance risks? The three main mitigation strategies are involving ourselves in the award process, identifying risk, and remediating risk. In the award stage of contract negotiations, ORC&S is the last step before a contract is awarded and funds are released to the PIs. The OSP contract administrators copy us on tickets to review proposals and the process halts until ORC&S responds saying the project is good to move forward a Technology Control Plan (TCP) around the project is required.

ORC&S developed a checklist for OSP administrators to reference in which if a certain box on the "IAS" form is marked as "yes," they go to a specific department. If the boxes "U.S. persons only", "Material Transfer Agreement", and "Non-Disclosure/Confidentiality Agreement" are marked as "yes", they automatically come to ORC&S for review. Specific agencies also automatically come to ORC&S for review. These agencies include Department of Agriculture, Department of Energy, Department of Defense, NASA, and NSF.

ORC&S has identified specific academic departments at MSU where the nature of their research creates inherent export risk. Therefore, awards and proposals from those department automatically come to ORC&S for review. The High Performance Computing Collaboratory (HPCC), Center for Advanced Vehicular Systems (CAVS), Bagley College of Engineering, Raspet, and Advanced Composite Institute (ACI). All of our TCPs come from these departments.

If ORC&S need to put a TCP in place, part of our risk assessment is to verify citizenship of each researcher, especially important if the project is "US persons (U.S. citizen and legal permanent residents) only." The first time a researcher is on an export-controlled project, the ECO must fill out the "Research Security Verification of Citizenship" form. To complete it, the researcher must bring in proof of citizenship, birth certificate or passport for U.S. citizens by birth, certificate of naturalization for naturalized U.S. citizens, green card for legal permanent residents, or a foreign passport if the researcher is utilizing a Full-Time Employee Exemption to work on a controlled project. All personnel *(regardless of citizenship status)* on TCPs are screened for security risks through our E2Open system.

MSU's Procurement Department screens all companies who export items and equipment to MSU. They screen for sanctions, anti-boycott risks, and several other potential risks. All international travel that MSU pays for, in part or whole, comes through ORC&S. Once it is logged into Concur, ORC&S is notified to review the travel for potential risks, especially if the travelers are involved in export-controlled projects.

The ECO coordinates with HPCC when the DFARS 7012 cybersecurity clause is invoked in a contract. HPCC has the only SP 800-171 NIST Compliant enclave on campus so it is where MSU houses all CUI and other protected data. HPCC works with the PI to finalize a compliant security plan to ensure all technical data is properly protected, which is then added into the TCP.

Element 3→ Export Authorization
Export authorization at MSU follows the BIS flowchart of:
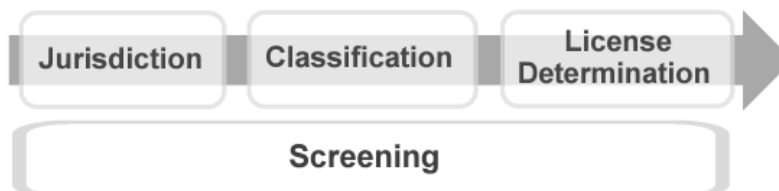
In the first step, ORC&S follows the order of review process. Is it ITAR? If not, is it EAR? If it's EAR but not controlled, it's EAR99. Once ORC&S figure out the jurisdiction, help is needed to classify the item. Our first step is always to reach out to the manufacturer for what they have on file. If they respond back negatively or do not respond, the ECO works in tandem with the researcher to classify. As the researcher is the subject matter expert (SME), the process works more efficiently with their help. If there is still no clear cut answer on what the classification is after this step, commodity jurisdiction submission to DDTC or BIS is needed for formal classification. Once ORC&S have a classification, they can turn to the reasons for control (if it is EAR) to ascertain if license is needed, and if so, what specific license.

Screening is the most important part of the process and should be performed throughout the course of the process. An entity ORC&S wants to export a piece of equipment to in May could very well be a denied entity when it is time to ship in December. The United States has shown many times how often they are willing to update their lists without warning so screeners must be cognizant of the ever changing geopolitical environment. All exporters have to ensure if they are passing on data or equipment (regardless of whether the data or equipment is controlled) to someone outside the United States, that they have clean backgrounds. All end-users are screened through E2Open. If they are rated as "approved", the export is good to continue. If they are rated as potential match (to someone who is on a denied list, such as OFAC sanctions lists, Commerce's Denied Entity List, etc.), which is usually either that is the same person or a similar/same name, some research is needed to ascertain exactly that. Are they the same person or do they just have similar or same names? If they clear, the transaction is clear to proceed..

Element 4→ Recordkeeping
ORC&S has dual record-keeping systems for maintaining TCPs, hard copy and electronic. Hard copies are found in the ECO's cabinet storage unit. Electronic copies of TCPs are found on the "Common" drive located in File Explorer. In additions to copies of TCPs, there are spreadsheets with all contract personnel on each project as well as a "Controlled Project Audit", which lists all export-controlled research projects, current and expired. Section 762.6 of the EAR mandates record keeping of all export-controlled research projects for five (5) years past the last date the projected performed any export-related activity. In addition, the Departments of State, Treasury, & Homeland Security all have their own separate recordkeeping requirements.

Element 5→ Training
Per MSU policy 70.04, every researcher who works on export-controlled projects at MSU must go through export control training. If they have never taken export control training before, they must take CITI Export Control training online. The online training has three modules and you must score a minimum combined score of 80% to pass the training and be able to work on export-controlled projects.

The initial CITI training is good for two (2) years and at the end of the two years, you are mandated to take a refresher briefing (which is currently being modified and updated by ORC&S). It is crucial to complete the refresher briefing before your two years are up. If your training expires and you are out-of-scope, you must re-take the initial CITI training.

ORC&S employees must take the initial CITI and refresher briefing trainings just like researchers on export-controlled projects. ORC&S employees also attend various webinars and outside training events

at universities across the country throughout the year. Moreover, the ECO is responsible for the export training program content and policy adherence.

Element 6→ Audit

There are two audit programs at ORC&S. One is conducted by the Assistant Security Coordinator monthly and one is conducted by the ECO annual. Monthly, the Coordinator monitors the funds associated with MSU export programs. The main goal is to verify that all researchers charging to the fund are eligible to do so, meaning they're up-to-date on training, are verified by ORC&S, and have signed the TCP for the project. If a researcher who is charging to a fund is missing one of the three aforementioned criteria, the Coordinator contacts the ECO. The ECO reaches out to the PI to verify they are still active on the project. If they are not active, the ECO marks it on the project spreadsheet and reaches out to the department to correct the charge. If they are active, the ECO reaches out to the researcher for them to complete the missing steps.

Additionally, the ECO conducts an annual export control audit on each project, usually in February. Each audit is broken down by PI and each project they lead. Prior to emailing the PI the ECO will verify the controlled project dates, modification, and funding amounts in Banner of each project. In an email to the PI to set up an appointment, the ECO emails them a sheet of 9 questions to review before meeting. The questions concern projects, dates, modifications, funding, personnel, etc.

Then, an email is sent to the PI (and co-PI's, if applicable) that states the reason for review with the audit checklist and personnel access list attached. The PI will answer the checklist items and consult with the ECO if any changes need to be updated in the TCP. The PI will also validate the personnel list is accurate as well. Once the review is complete the ECO files a signed copy in the respective TCP folders. This is repeated for each TCP. As part of the annual audit of the TCP, the ECO makes a visit to the facility and ensure all security protocols are being followed. The ECO shall provide the facility with at least two (2) weeks' notice of the impending visit.

If the PI has questions or concerns about the physical security implementation, the PI and ORC&S can work together to come up with a reasonable solution to the question or concern. Questions or concerns about data/information security can be brought to HPC2 and they can work in tandem to come up with a reasonable solution to the question or concern.

Element 7→ Handling Export Violations & Taking Corrective Actions

The best way to act upon an export violation is to detect it and act on it early. Quick responses help minimize MSU's exposure to more severe export violation punishments. Support from senior management is crucial. Export compliance, particularly at universities but also anywhere else, only functions properly when there is commitment stemming from the top of the food chain all the way down to undergraduate researchers.

Researchers are encouraged to reported suspected export violations and it is a part of the researching duties to do so. Reporting export violations can help MSU stay out in front to correct the violation quickly. If there is a violation, the continuity of federal funding for export-controlled research may hinge on how quickly and accurate MSU can correct the violation.

There are multiple ways to report a violation. To report a violation overtly, you can contact the ECO or anyone else at ORC&S. If you prefer to submit a report anonymously, you can go to the MSU Ethics Point website, https://secure.ethicspoint.com/domain/media/en/gui/24520/index.html. From there, you can click on: Make a Report→ Research→Research Security/Export Control