FLORIDA STATE UNIVERSITY

CERTIFICATION ON THE HANDLING OF

EXPORT CONTROLLED INFORMATION

**Overview:** The research project identified below will involve the receipt and/or use of technical data that is controlled under United States export control laws: the Export Administration Act and Export Administration Regulations (“EAR”), enforced by the Bureau of Industry and Security in the Department of Commerce or the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations (“ITAR”), enforced by the Office of Defense Trade Controls in the State Department.

**ITAR:** The ITAR control the export of equipment, technologies and technical data that are primarily military in nature. It is unlawful under the ITAR to send ITAR controlled technical data to *any* foreign persons outside the United States or to disclose – in written, oral or visual form -- ITAR- controlled technical data to *any* foreign persons *in* or *outside* the United States unless one of several exclusions applies or the State Department has issued a license authorizing the disclosure or export of the technical data to specific foreign persons.

**EAR:** The EAR control the export of equipment, technologies (including software), and technical data that serve primarily civil uses. The prohibition on the export or disclosure of technical data controlled under the EAR is determined on a country-by-country basis for each disclosure of controlled technical data. As a result, it is unlawful to export technical data out of the US or to disclose technical data in or outside the US to foreign persons of countries for which a license is required as a condition of making such exports and disclosures.

**Definitions:**

A **“foreign person”** is anyone who is “not a lawful permanent resident” of the United States (i.e., not a green card holder) or does not have refugee or asylum status.

In general, **export controlled technical data** is specific information that is needed to develop, produce, maintain, manufacture, assemble, test, repair, operate, modify, process or otherwise use equipment or technologies that are on the control lists of the EAR or the ITAR. Controlled technical data may take the form of “blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.” Basic marketing information on function or purpose of equipment; general system descriptions; general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities and related information, and information that is in the public domain -- commonly available to interested persons – does not qualify as controlled technical data under the export control laws. The export laws and regulations determine if technical data is controlled, not your intended or actual use of the information.

**Obligations:** Recipients of export controlled technical data may be held personally liable for disclosures of export-controlled technical data to unauthorized foreign persons. As a result, researchers must take reasonable measures to prevent the disclosure to and use and access of export- controlled technical data by unauthorized, unlicensed foreign persons. What qualifies as reasonable depends on the circumstances. Examples of measures researchers should consider adopting include clearly marking “controlled” technical data that is controlled, identifying personnel who may lawfully access the technical data, storing hard copies of controlled technical data in locked cabinets or desks, securing access to electronic copies of and communications containing controlled technical data by passwords, user ids, or other controls; storing technical data in a single location; making only that number of copies of technical data as is necessary, and requiring all persons with lawful access to controlled technical data to sign this certification.

**Penalties:** Generally, any person or entity that brokers, exports, or attempts to export a controlled item without prior authorization, or in violation of the terms of a license, is subject to penalties. Violators may incur both criminal and civil penalties.

**ITAR Violations**

The Arms Export Controls Act (AECA) and the International Traffic in Arms Regulation (ITAR) provide that willful violations of the defense controls can be fined up to $1,000,000 per violation, or ten years of imprisonment, or both. In addition, the Secretary of State may assess civil penalties, which may not exceed $500,000 per violation. The civil penalties may be imposed either in addition to, or in lieu of, any other liability or penalty.

**EAR and Anti-Boycott Violations**

Similar to the ITAR, violations of the Export Administration Regulation (EAR) are subject to both criminal and administrative penalties.  Fines for export violations, including anti-boycott violations, can reach up to $1,000,000 per violation in criminal cases, and $250,000 per violation in most administrative cases.  In addition, criminal violators may be sentenced to prison time up to 20 years and administrative penalties may include the denial of export privileges.

**OFAC Violations**

Although potential penalties for violations of U.S. export laws vary depending on the country and material involved, an exporter may be subject to a maximum civil penalty of $250,000 per violation under the Office of Foreign Assets Control regulation.

**Researcher Certification:** I certify that I am familiar with the export control issues summarized above and have read and understand this certification. I understand that I could be held personally liable if I unlawfully disclose export controlled technical data to foreign persons and agree to take reasonable measures to prevent unauthorized foreign persons from having access to or using any export controlled technical data I may receive under the contract identified below. I agree to take appropriate security measures and to contact the FSU Office of Research Compliance Programs, identified below, before making any type of disclosure of controlled technical data to any foreign person.

Signature of Researcher       Date:

Printed Name of Researcher:

Department:

Research Project Title:

OMNI Project ID#

RAMP Export Control Request ID:

Funding Agency:

**Submit completed certification** to the Office of Research Compliance Programs at [research-compliance@fsu.edu](mailto:research-compliance@fsu.edu). For questions, email [dkey@fsu.edu](mailto:dkey@fsu.edu) or call (850) 644-8648.

For additional information on export controls, visit

* [Bureau of Industry and Security website](https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear)
* [Office of Defense Trade Controls website](https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987)
* [FSU’s Export Controls website](https://www.research.fsu.edu/research-compliance/export-controls)