CERTIFICATION FOR HANDLING 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); the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations (ITAR); the Office of Foreign Assets Control (OFAC) sanctioned countries programs; or the Department of Energy's (DOE) controls on nuclear activities. For additional information on the above export regulations click on the agency name: EAR ,ITAR, OFAC, DOE

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 and access of export-controlled technical data by unauthorized unlicensed foreign persons defined as anyone who is "not a lawful permanent resident" of the United States (i.e. not a green card holder). Researchers on this contract shall clearly mark export controlled technical data, identifying personnel who may lawfully access the technical data, store hard copies of controlled technical data in locked cabinets or desks, secure access to electronic copies of a communications containing controlled technical data by passwords, user ids, or other controls; store technical data in a single location and require all persons with lawful access to controlled technical data to confirm their understanding and agree to these conditions. See recommended security guidelines below.

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 as outlined below to prevent unauthorized foreign persons from having access to or using any export controlled technical data I may receive under the agreement identified below.

Signature of Researcher _____ Date _____

Print Name of Researcher _____ Dept _____

Project Title _____

Sponsor _____ Proposal/ Account # _____

Send completed form to ASU Research Operations by email research.integrity@asu.edu, or campus mail code 6011. Keep a copy for your project file. (Note: Government regulations require that all records be kept for five years.)

For questions about this form or other export matters contact ASU Research Operations at research.integrity@asu.edu.

GUIDELINES FOR THE PROTECTIVE SECURITY OF TECHNICAL INFORMATION/DATA, MATERIALS AND EQUIPMENT THAT ARE EXPORT CONTROLLED.

Project security is the responsibility of the Principal Investigator (PI). Specifically, technical information, data, materials, software or hardware, i.e., technology, generated from export controlled contract or subcontract will be secured from use and observation by non-U.S. citizens. Examples of some methods to provide this security are as follows:

- **Project Personnel** – The use of security badges may be necessary as an aid to identify personnel whose access to project facilities and work in progress is authorized.
- **Laboratory "work in progress"** – Project data and/or materials must be physically shielded from observation by unauthorized individual by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- **Work Products** – Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets, preferably located in rooms with key – controlled access.
- **Equipment or internal components** – Such tangible items and associated operating manuals and schematic diagrams containing identified "export controlled" technology are to be physically secured from unauthorized access.
- **Electronic communications and databases** – Database access will be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using federally approved encryption technology. Communications via telephone must have similar encryption capability.
- **Conversations** – Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only conducted under signed confidentiality agreements and fully respect the Non-U.S. limitations for such disclosures.

  Note: Non-Disclosure Agreements are negotiated through ORSPA contracts and may require formal approval of the federal Contracting Officer.

Principal Investigators are reminded that sponsor restrictions on the publication or public disclosure of technical information, data, materials, or software generated under an export-controlled contract must have a publication waiver approved by the KE Research Operations authorized official prior to commencing any work.

The penalty for unlawful export and disclosure of Export-Controlled Information under the ITAR, EAR or OFAC can be severe. Criminal and civil penalties can be monetary (e.g. up to $1 million per violation), prison time (e.g. up to 20 years), or both, and Debarment. For more information see ITAR penalties, OFAC Civil penalties and Enforcement Information, and EAR penalties.

Definitions:

Foreign Person: Foreign governments, foreign corporations and their representatives, as well as citizens of foreign countries.

U.S. Person: Includes United States citizens and "Green-Card" holders, permanent resident aliens. It also includes any corporation, business association, partnership, society, trust, or any other entity organization or group that is incorporated to do business in the United States.