****RSP130 (11/2019)

**ACKNOWLEDGEMENT OF BRIEFING AND HANDLING OF**

**EXPORT CONTROLLED INFORMATION**

This project involves the use of Export-Controlled Information. As a result, the project implicates either the International Traffic in Arms Regulation (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.

It is unlawful under the ITAR to send or take Export-Controlled Information out of the U.S.; disclose, orally or visually, or transfer export-controlled information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, a license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

In general, Export-Controlled Information means activities, items and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing or use of items with a capacity for military utility. Export-Controlled Information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export-Controlled Information is military or civil in nature.

Researchers may be held personally liable for violations of the ITAR and EAR. As a result, you should exercise care in using and sharing Export-Controlled Information with others. Technical information, data, materials, software or hardware, i.e.; technology generated from this project, must be secured from use and observation by unlicensed non-U.S. citizens. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including incarceration.

Security measures will be appropriate to the classification. Examples of security measures are (but not limited to):

* Project Personnel – Authorized personnel must be clearly identified.
* Laboratory “work-in-progress” – Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
* Marking of Export-Controlled Information – Export-Controlled Information must be clearly identified and marked as export-controlled.
* 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.
* Electronic 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 – Appropriate measures will be taken to secure controlled electronic information. Such measures may include: user ID, password control, or approved encryption technology. Database access may 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 a federally approved encryption technology.
* Conversations – Discussion about the project or work products are limited to the identified contributing investigators and are only in areas where unauthorized personnel are not present. Discussion with third party sub-contractors are only to be conducted under signed agreement that fully respect the non-U.S. citizen limitations for such disclosures.

Research Project Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PI/Departments:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sponsor:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Certification:** I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined in the TCP. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled Information to unauthorized persons.

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_