# Old Dominion University

### Part II: Briefing and Certification on the Handling of Export-Controlled Information

This project involves the use of U.S Export-Controlled information, equipment, or software. As a result, the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), or other U.S. Export-Control regulations apply to the project.

the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, processing, or use of a controlled item requires an export license, or license exception, to physically export from the U.S. OR to discuss with or disclose to a person who is not a U.S citizen or lawful permanent U.S resident. The ultimate end-use or end-user of the information, software, or item is not determinative of whether it is Export-Controlled.

Basic marketing information on function or purpose; general system descriptions; information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities; published information in the public domain; and published patent information is not Export-Controlled. Information developed as a result of fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published, without any publication restriction or pre-publication review requirement is not Export-Controlled.

It is unlawful to send or take Export-Controlled information, technology, software, or items out of the U.S; or disclose, orally or visually (including by email, fax, phone, etc.), or transfer to a foreign person inside or outside the U.S without prior authorization from the cognizant U.S government agency. A foreign person is a person who is not a U.S citizen or lawful permanent resident alien of the U.S. A person lawfully in the U.S on a visa for work or study is a foreign person. The law makes no exceptions for foreign graduate students or visiting scientists.

Researchers may be held personally liable for civil or criminal violations of the U.S. Export-Control Regulations. As a result, you should be dear on the requirements and exercise reasonable care in using and sharing Export-Controlled information, technology, software, or items with others. This Technology Control Plan is to help you assess, address, understand your obligations, and control access to the Export-Controlled aspects of this project.

The security measures you design and implement should be appropriate to the type, nature, and level of Export-Controlled information, technology, software, and/or items involved in the project. Examples of appropriate security measures include (but not limited to):

<u>Project Personnel</u> - Authorized personnel must be dearly identified.

-in- ons,on-

Discussions with third party sub-contractors are only to be conducted undefully respect the non-U.S citizen limitations for such disclosures.	er signed agreementsthat
Controlled data or information should be loaded to, sent to, or stored on a device. See the provision on Information Security below.	No Export- ny personal electronic
NT AND EXECUTE THIS <u>CERTIFICATION</u> FOR EACH PERSON WHO WILL HAVE ACCESS TO EXPO	RTCONTROLLED SUBJECTMATTE

### Part III: Technology Control Plan (TOP)

### 1 Commitment

Old Dominion University (ODU) and Old Dominion University Research Foundation (ODURF) are committed to export controls compliance. The Principal Investigator is responsible for implementation of technology control plans. The ODU Office of Research is responsible for assessing the adequacy of technology control plans, as applicable. The Export Control Officer is Adam Rubenstein. Julian Facenda, Executive Director, ODURF and Adam Rubenstein, Ph.D., Assistant Vice President for Research Compliance, are both Empowered Officials who may approve this Technology Control Plan. The Export Controls Officer is the main contact for export control issues.

The individual responsible for and committed to ensuring compliance with this TCP is:

5	Personner screening
	All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form.
6	Training and Awareness
	All personnel with access to Export-Controlled information, technology, software, or items on this project have read and understand the riefing and Certification on the Handling of Export - Export control training modules are available and additional export control training for this project may be conducted by the Export Controls Officer. Additionally, all personnel with access to digital data/information stored on their university computer have read and agree to follow ODU policies and procedures for protecting sensitive data.
7	Compliance Assessment
	oing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Export Control Officer at <a href="mailto:arubenst@odu.edu">arubenst@odu.edu</a> (757.683.3686) or to the ODURF Executive Director at <a href="mailto:jfacenda@odu.edu">jfacenda@odu.edu</a> (757.683.4293, ext. 600). The Export Controls Officer and the Information Security Office may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Export Control Officer.
8	Project Termination
	Security measures will be required for Export Controlled information and items after the project termination. Please describe the security measures to remain in effect for Export Controlled information and items following termination of the project as well as the document retention and disposition plan to be followed:

## 9 Changesto Personnel

In the event thatic Tm0 g3 Tm0 g0 (a) 17()52.1g3 Tm0 612 792 reW\*nBT40 1 246.73 373.18 Tm0 12 792 re- (b) -20(le) 36(a) 110(j) 8