Briefing Verification Form for Handling Export Controlled Information

You are being briefed on the requirements for controlling information or material because a project you are involved in is controlled under the State Department’s International Traffic in Arms Regulations (ITAR) or the Commerce Department’s Export Administration Regulations (EAR). The accompanying Technology Control Plan (TCP) and Non-Disclosure Agreement (NDA) must be signed by all persons authorized to have access to the information or materials to verify you understand the requirements to protect the information and/or material(s), and to accept the responsibility to secure them at all times from transfer to any unauthorized foreign nationals within or outside of the U.S. The Office of Institutional Compliance keeps these records on file.

It is unlawful under the ITAR and EAR to send or take export controlled information out of the U.S., or to disclose or transfer export controlled information to a foreign person in the U.S. without proper authorization. Depending on the nature of the material or information and the jurisdiction (ITAR or EAR), a license might be required for foreign person 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 students.

An export is defined as any of the following: 1) actual shipment of any covered goods or items from the U.S. 2) the electronic or digital transmission of any covered technology or item from the U.S.; 3) any release or disclosure, including verbal disclosures or visual inspections, of any controlled technology, software or technical data to any foreign nationals; or actual use or application of controlled technology on behalf of or for the benefit of any foreign entity or person anywhere. In general, export controls apply to items on the Commerce Control List (under the EAR) and the U.S. Munitions List (under the ITAR). You should be familiar with the categories and items on each list that relate to your specific discipline. 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 in nature or not.

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. persons. Security measures will be appropriate to the classification involved. Examples of security measures are:

- **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.
- **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** - Appropriate measures will be taken to secure controlled electronic information. Such measures may include: User ID, password control, SSL or other 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 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- **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 to be conducted under signed agreements that fully respect the non-U.S. person limitations for such disclosures.
Each project that is subject to export control regulations must have an approved Technology Control Plan (TCP) in place that outlines the procedures to handle and safeguard the export controlled information before the work may be accepted at UML. It is the responsibility of the Principal Investigator to develop a written TCP. The PI and each person working on the project must be U.S. persons and provide proof of citizenship as requested. All persons involved must review the TCP, including the employee responsibilities and nondisclosure agreement, and then sign the NDA and TCP. An authorized member of the Office of Institutional Compliance also signs the TCP to indicate that the TCP is acceptable, and that personnel have been briefed about their responsibilities.

Signed documents are kept on file with the Office of Institutional Compliance. For assistance contact Thomas_Porro@uml.edu at ext. 4-3207 or Elaine_Major@uml.edu at ext. 4-3452.