Briefing on the Handling of Export-Controlled Information

For projects that include the use of Export-Controlled Information, the project falls under either the State Department's International Traffic in Arms Regulations (ITAR) or the Commerce Department's Export Administration Regulations (EAR).

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 application 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.

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. 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. citizen limitations for such disclosures.

Each project subject to export controls must have a Technology Control Plan (TCP) in place that outlines the procedures to be taken to handle and safeguard the Export-Controlled Information. It is the responsibility of the Principal Investigator (PI) to develop a written TCP which must be approved and signed by the Vice Chancellor of Research or Executive Director of Administration and Finance. The PI must ensure each person working on the project has read and understands the **Briefing on the Handling of Export Controlled Information** and has read and understands the TCP. Project personnel must sign the **Technology Control Plan Certification** before they can begin work on the project. Pending the hiring of the Director of Research Compliance, return the signed document to Joanne Zanella-Litke, Director, Office of Research Administration, Room 011, Foster Admin Bldg.. For assistance call ext. 8942 or email jzanella@umassd.edu. Forms are available under Export Controls at http://www.umassd.edu/grants_contracts/compliance/export. A copy of the final signed TCP and Certification form will be returned to the PI.