Technology / Export Control Plan (T/ECP)

This project/activity involves the use of Export-Controlled Information (ECI). As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR) or the Department of Commerce's Export Administration Regulations (EAR)

It is unlawful under the EAR or ITAR to send or take Export-Controlled items or information out of the U.S. This includes disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, an export 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.

Pertinent technical information, data, materials, software, hardware, i.e. technology generated from this project, must be secured from use and / or observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved.

In order to prevent unauthorized exportation of protected items / products, information, or technology deemed to be sensitive to National Security or economic interests, a Technology / Export Control Plan (T/ECP) may be required. If so, this is a basic template for minimum elements of a T/ECP.

T

1. Physical Security Plan: (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. This would pertain to laboratory management of "work-in-progress")

   a. Location (describe the physical location of each sensitive technology / item to include building and room numbers. A schematic of the immediate location is highly recommended):

      x

   b. Physical Security (provide a detailed description of your physical security plan designed to protect your item/technology form unauthorized access, ie., secure doors, limited access, security badges, CCTV, etc.):

      x

   c. Perimeter Security Provisions (describe perimeter security features of the location of the protected technology / item):

      x

2. Information Security Plan (Appropriate measures must taken to secure controlled electronic information, including User ID's, password control, SSL or other approved encryption technology. Database access must be managed via a Virtual Private Network (VPN), allowing only authorized persons to access and transmit data over the internet, using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology).

   a. Structure of IT security (describe the information technology (IT) setup / system at each technology / item location:

      x

   b. IT Security Plan (describe in detail your security plan, i.e., password access, firewall protection plans, encryption, etc.):

      x

   c. Verification of Technology/Item Authorization (describe how you are going to manage security on export controlled materials in the case of terminated employees, individuals working on new projects, etc.):

      x

   d. Conversation Security (Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors are only to be conducted under signed agreements that fully respect the U.S. non-citizen limitations for such disclosures. Describe your plan for protecting export controlled information in conversations):

- x

3. Item Security

   a. Item Marking (Export controlled information must be clearly identified and marked as such):

      - x

   b. Item Storage (Both soft and hard copy data, notebooks, reports and research materials are stored in locked cabinets, preferably in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing “export-controlled” technology are to be physically secured from unauthorized access):

      - x

4. Project Personnel (clearly identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology / item).

Name:

Name:

Name:

5. Personnel Screening Procedures

   a. At a minimum, you must review entities and denied parties list found on the Department of Commerce web site at http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm.

b. U.S. Employees (describe training for U.S. employees with access to controlled technology areas.

- x