Export Controls and Proprietary Technical Information

- *Receiving proprietary or sensitive technical information from an outside source such as a government or industry sponsor?*
- *Storing technical information on your hard drive or other devices?*
- *Traveling to a foreign location?*

A basic understanding of the export regulations related to technical information can help you prevent a violation during research and travel activities.

Key Concepts in export control:

Export control laws apply to both military and commercial technologies. More information on the laws can be found at: www.umresearch.umd.edu/Export/exportlaws.html

Technical information is defined in export laws as *information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of an article.*

A **"deemed export"** involves sharing export controlled technical information with a non-US person (in any location and by any means) or taking it out of the country on a device. For example, providing export-controlled information to a foreign national in your lab could be considered a deemed export. If the technical information relates to a controlled technology, an export license may be required depending on the technology, location, or nationality of the receiving person.

University research data is typically exempt from export control if it is conducted with the intent to publish (i.e. fundamental research).

Proprietary data (typically furnished from outside sources) is not exempt from export control. Even if conducting fundamental research, data received from outside sources may be subject to export controls.

Export-controlled technical information is proprietary information that is related to an item subject to control under US export laws. Export-controlled technical information has restrictions on who can access it, and where it can be stored or sent. The level of control varies depending on the nature of the associated item.

Cloud service providers such as Google Apps often use non-US servers and cannot be utilized to store or transmit controlled technical information unless they are certified for US-only server locations. UMD's version of Box can be utilized under certain circumstances to store export-controlled information. Contact the ECO for more information.

Export Controls and Proprietary Technical Information

DoD-Funded contracts have special contractually mandated requirements for handling of controlled technical information.

Guidance for faculty and staff:

1. **Travel Clean.** Proprietary technical data should not be stored on any electronic devices (phones, laptops) if you plan on traveling internationally with the device. For this reason, it is not recommended that you travel with a hard drive used to store your regular emails and files. More travel guidance can be found at: www.umresearch.umd.edu/Export/internationaltravel.html

2. **Avoid Receiving Proprietary Technical Data**. During early engagements with potential sponsors or collaborative parties, remind your technical counterparts not to send proprietary technical data. If absolutely necessary to receive proprietary information, ask whether the information will be subject to export controls. It is recommended that you establish a Non-Disclosure Agreement (NDA) which must be executed by a University official. Brian Falasca (bfalasca@umd.edu) can be contacted with any questions pertaining to NDAs.

3. **Review incoming information for restrictive markings.** Any time you receive proprietary technical data from an outside source, review the material for restrictive markings which may indicate the material is export-controlled. If no markings are provided, you may consider asking the source to confirm that the material is not export-controlled.

4. **If you receive export-controlled information, contact the Export Compliance Office (ECO) for guidance**. The ECO can help determine how the material may be used and who may have access to it. A Technology Control Plan (TCP) can be created to help manage the data securely. The data must not be stored on an unrestricted server location. If you are not a US citizen or permanent resident, you may not access the data until the level of export control can be determined. The ECO is available to assist with that determination.

5. **Understand the restrictions for storing and sending export-controlled data.** Email should NOT be used for transmitting or storing export-controlled information. Work with the sender and/or the Export Compliance Office to determine a secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive. External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use. Drives and devices used to store export-controlled information must be password protected or encrypted.

6. **Need an export license?** In certain circumstances, the ECO can apply for an export license to allow shipment of export controlled technology or data, or for a foreign person to have access to controlled information. Licenses require a lead time (3+ months). Contact the ECO as soon as possible if the need arises.