# The Devil is in the Details: Documenting Export Controls Compliance

Kay Ellis
Associate Director, Export Controls Officer
Office of Sponsored Projects
University of Texas at Austin

6th Conference for Effective Compliance Systems in Higher Education
Austin, TX
June 2, 2008

# Export Control Licenses and Technology Control Plans (TCPs)

- Department of Commerce Bureau of Industry and Security grants licenses to
  - Ship certain items outside the U.S.
  - Give controlled technology to a foreign national (deemed export license)
- Department of State grants licenses to
  - Ship certain items outside the U.S.
  - Provide a defense service to a non U.S. person
- OFAC grants licenses for
  - Payments, services, travel, or shipments to certain countries

# What is a Technology Control Plan?

- A TCP is simply a plan that outlines the procedures to secure controlled technology (e.g., technical information, data, materials, software, or hardware) from use and observation by unlicensed non-U.S. citizens.

# When do you need a TCP?

- In conjunction with a Technical Assistance Agreement (TAA) – Dept. of State
- In conjunction with a Deemed Export license – Dept. of Commerce
- In conjunction with an agreement that does not allow foreign nationals
- In conjunction with an agreement that involves controlled technology – includes NDAs
- Or in conjunction with ***any*** project that involves controlled technology!

# What are some key elements to consider in developing a TCP?

- **A TCP is project-specific!**
- Authorized personnel should be identified
- Export-controlled information must be identified and marked as export-controlled
- Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured lab spaces or time blocks
- Work products such as soft and hardcopy data, lab notebooks, reports, and research materials should be stored in locked cabinets preferably in rooms with key-controlled access

# More elements to consider…..

- Key controlled access by authorized personnel only
- Equipment or internal components such as operating manuals and schematic diagrams containing identified export-controlled technology must be secured
- Disposal of export-controlled information
- Discussions about the project
  - authorized personnel only and in secure area
  - no third-party discussion unless conducted under signed agreement with U.S. citizen limitations

# Even more elements to consider…..

- Export-controlled electronic communications and databases need to be secured. Such measures may include:
  - user ID, strong password, SSL or other approved encryption technology (TrueCrypt)
  - activate screensavers after 10 minutes
  - full disk encryption for laptops
  - procedures for Protecting Sensitive Digital Research Data found at http://www.utexas.edu/its/policies/researchers/index.php

# How we handle TCPs at UT Austin

- Most (but not always!) TCPS are implemented at the award stage
  - Some Non-disclosure agreements require a TCP
- Before work can begin on the project, PI completes TCP Certification forms
  - PI lists project personnel, sponsor, and area/category of export control (Department of State or Commerce)
  - Project-specific TCP developed
  - All project personnel sign Certification
  - Export Control Officer signs

# Now that the TCP is in place…

- Project personnel need to be trained or briefed prior to the start of the project
- Update Certification every semester – project personnel could change
- Retrain project personnel at least once a year
- Audit project to make sure TCP is being followed

# Now that the project is over… recordkeeping requirements

- Departments of State and Commerce require documentation be kept five years after the expiration of license
- Even if a license is not involved, documentation should be kept the life of the project and at least five years after the project ends
- Security measures should remain in effect to protect export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer controlled.

# Now that the project is over… recordkeeping requirements

- Destruction of records allowed by the Bureau of Industry & Security (BIS) after five (5) years except
  - Records of Voluntary Self Disclosures require BIS approval
  - Records previously requested by BIS require BIS approval
- Records to be retained required by the Department of State
  - Registration records
  - Exemption records

# A word about OFAC

- The Office of Foreign Assets Control (OFAC) licenses are only valid for one year from the date of signature by OFAC
- Recordkeeping requirement in the text of the license: 5 years

# Voluntary Disclosures

- If you realize a violation has occurred, the appropriate agency should be notified
  - Penalty may be less severe
- What, When, Who, Where, and Why – investigate, research, compile facts
  - What was the general nature of the violation and what item was involved
  - When did it occur – timeframe
  - Who was involved – parties to the export
  - Where did it occur – U.S., overseas
  - Why did it occur – were policies adequate?

# Voluntary Disclosures

- Need to show corrective action taken and the measures put in place to prevent it from happening again
  - Root causes identified and addressed
  - Remedial training provided
  - Policies & procedures reviewed and addressed
- Provide all relevant documentation and submit disclosure

# Questions or Comments?

Kay Ellis
The University of Texas at Austin
512-475-7963
kay.ellis@austin.utexas.edu