Export Compliance Guidelines
for
Safeguarding Export Controlled Technical Data

Export controlled technical data housed at UCAR/NCAR should be managed in accordance with these guidelines.

A project specific Technology Control Plan (TCP) is required for all projects that involve the use of export controlled technical data.

Technology Control Plan (TCP)

All UCAR projects that have Export Controlled Technical Data must have a Technology Control Plan (TCP) in place. The TCP shall include all requirements that the funding source specifies. At a minimum, the TCP will address the following aspects of safeguarding ECTD: Authorized personnel, physical security, information security, and training.

The purpose of a TCP is to control the access and dissemination of export controlled technical data in accordance with federal export regulations by ensuring that everyone working on an export controlled project understands their obligations under export control laws and regulations. A TCP template can be found here: http://www2.fin.ucar.edu/sites/default/files/TCP%20Template2013.docx

Establishing a TCP is a multi-step process where: 1) the PI develops the TCP in coordination with the Export Compliance Coordinator (ECC) and submits it to the Export Compliance Manager (ECM); 2) once approved, the PI is responsible for reviewing the control plan with all participants who individually sign off that the plan has been explained to them; 3) the PI submits a copy of all signed documents to the ECC and ECM, and keeps the originals with the project file, and implements TCP; 4) the PI notifies the ECC and ECM of any updates to the TCP as they occur (personnel, scope of work, safeguards, etc). All staff who are accessing or handling export controlled technical data, including IT and SysAdmin staff, are required to be included in the TCP.

Access Controls

- Do not access Export Controlled Technical Data from shared, public computers such as kiosk computer in libraries, hotels, and business centers, or from computers that have no local access control.
- Do not post Export Controlled Technical Data on public websites or websites that rely solely on IP addresses for access control. Instead, secure access by using individually
Export Compliance Guidelines
for
Safeguarding Export Controlled Technical Data

assigned accounts requiring username/password, user certificates, or other user-specific
authentication methods.

- Protect Export Controlled Technical Data by at least one physical and one electronic
  barrier (e.g., locked container or room and login with password) when not under direct
  individual control. Unless specifically configured, a UCAR office does not provide a
  sufficient physical barrier.

Labeling

Systems and devices that host Export Controlled Technical Data need to be clearly labeled so
that everybody can handle them correctly. Ideally, the label should indicate which export
control regulation governs the technical data (e.g., ITAR, EAR). Labeling should include:

- A physical label on devices that have Export Controlled Technical Data on the (e.g.,
  laptop, external drive)
- A physical label on racks in computer rooms that house systems with Export Controlled
  Technical Data
- A logon or service access banner presented when a user logs in to any system with
  Export Controlled Technical Data.

Suggested label/login text:

WARNING – This document contains technical data whose export is restricted by the Arms
Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979,
as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to
severe criminal penalties.

System Management

- The system must be kept up to date on security patches and updates, and must use
  regularly updated malware protection software.
- UCAR systems with ECTD stored on them are managed by the IT department for the lab
  housing the project with ECTD. User Managed devices (as specified in the TCP) must also
  adhere to the guidelines and must be available as needed or on schedules to the IT
  department for log analysis/offload, patch assurance, and system vetting.
- Only devices and persons included in the TCP are authorized to hold and access ECTD.
Export Compliance Guidelines
for
Safeguarding Export Controlled Technical Data

- All ECTD must be encrypted if stored on mobile computing devices such as laptops, and on removable media such as thumb drives or CDs/DVDs. See additional notes below.
- Users should work with their IT department to dispose of all media/disks with ECTD. Unless otherwise specified in the TCP, media/disks are sent to a data destruction company with chain of custody and certification of destruction.

Transmission of ECTD

- Export Controlled Technical Data cannot be emailed or stored using any of the Google Apps for Government.
- Transmit ECTD using only the approved methods detailed in the TCP.
- ECTD on the internal UCAR network must be encrypted in transit.
- Transmit ECTD via voice or fax only between authorized people in the TCP.
- Transfer ECTD only to subcontractors and collaborators listed in the TCP.

Storing ECTD

- Export Controlled Technical Data is stored only on devices listed in the TCP.
- ECTD stored on an authorized system in secure locations such as a locked rack in a controlled access data center do not have to be encrypted.

Shipping

Following UCAR Policy 1-6, all international shipments of items and export controlled documents and technical data on media must be routed through Logistics. Technical data electronic transfers pursuant to existing Technical Assistance Agreements (TAAs), and documents that are not subject to export controls are the only exceptions.

Mobile Computing Devices

The use of laptops, tablets, cell phones, and other removable storage devices must follow strict guidelines that are detailed in an approved TCP.

Google Apps for Government

Google's terms and conditions strictly prohibit using Gmail, Google Drive, and any Google Apps for Gov for emailing, sharing, transferring or storing Export Controlled Technical Data.
Export Compliance Guidelines

for

Safeguarding Export Controlled Technical Data

(ECTD). ECTD must be handled in accordance with U.S. export control laws and regulations at all times. Researchers and others handling ECTD must take reasonable measures to prevent the disclosure, use, and access of export controlled technical data by unauthorized, unlicensed foreign persons.

NCAR/CISL Supercomputers and data storage (e.g., HPSS)

The NCAR/CISL supercomputers and data storage (e.g., HPSS) cannot be used for transfer, processing, sharing or storage of ECTD.