Fermilab | U.S. DEPARTMENT OF ENERGY | Office of Science

Export Control Awareness and Basic Cybersecurity Training for Fermilab Visitors

Agenda

- What is an Export?
- Export Control Restrictions
  - Who? What? Why?
  - Dual-Use Items
  - Fundamental Research Exclusion (FRE)
- Fermilab's Export Control Policy
- Export Control Roles
- Applying Export Controls to Fermilab
- Export Control Review Prior to Public Release of Information
- Resources
- Quiz

What is an Export?

- Transferring controlled items:
  - Hardware (e.g., equipment, raw materials, etc.), **OR**
  - Software, **OR**
  - Technology (e.g., design documents, repair manuals, etc.)
- Verbally, Visually, Physically, or Electronically
- To either:
  - Another country, **OR**
  - A foreign national (even in the U.S.), **OR**
  - A foreign institution

- **Some transfers may require a license or Export/Import ("Ex/Im") Compliance approval PRIOR to export**

What is an Export?

- For Export Control purposes, there are two categories of people:
  - U.S. Person: U.S. citizen, U.S. lawful permanent resident (i.e., “green card” holder), and some protected persons
  - Foreign National: Anyone who is not a U.S. person. Holders of nonimmigrant visas are foreign nationals
- Releasing, furnishing, showing or disclosing export controlled technical information or source code to a foreign national, even in the US is a **“deemed export”**

What is an Export?

Deemed exports may include:

- Allowing photography, videography, or visual inspection by a foreign national that reveals details of the design or manufacturing process
- Mail/Email/Social media available to foreign nationals
- Uploading code or design data to a public website
- Transferring a laptop, flash drive, cell phone, or paper to a foreign national
- Detailed discussion about software, technical designs, practical applications, manufacturing, or repair of controlled items during meetings, presentations, or conferences

Who Administers Export Control Laws & Regulations?

- **Department of Commerce** – Export Administration Regulations (EAR), 15 CFR 730-774
  - Controls most dual-use exports
- **Department of State** – International Traffic in Arms Regulations (ITAR), 22 CFR 120-130
  - Controls defense articles and services
- **Department of Treasury** – 31 CFR 500
  - Administers most economic sanctions
- **Department of Energy** – 10 CFR 810
  - Controls specific emerging technologies (DOE O 485.1A)
  - Controls unclassified nuclear technology & assistance

What are Some Export Control Restrictions?

- Export Control laws control the export of dual-use, emerging, defense items, and technology
  - Ex/Im Compliance determines if items and technology are controlled and provides guidance
  - Ex/Im Compliance determines if licenses, exceptions, or exclusions apply
- Export Control laws prohibit some transactions with specific countries, entities, and/or individuals
  - Ex/Im Compliance determines if these restrictions apply and provides guidance

Why Comply?

- **It's the law** – applies to Federal laboratories
- **Prime Contract Clause I.101C (flow down)**
  - DEAR 970.5225-1
- Fermilab's robust collaborates with:
  - Foreign governments, institutions;
  - Expert foreign nationals; and
  - Hosting users and visitors from many foreign institutions (*>35% of users are from institutions outside USA*)
- Consequences of non-compliance
  - Civil penalties ($250,000 - $1M per violation)
  - Criminal penalties (fines; **jail for individuals**)
  - Loss of prime contract & negative publicity

Why Comply?

- Former University Of Tennessee Professor John Reece Roth
  - Worked with national laboratories
  - 4 year prison sentence for illegally exporting military research data (2012)
- During course of a contract:
  - Allowed 2 foreign students to access export controlled data and equipment
  - Foreign students took some data to China
- *"This sentence communicates the importance of export compliance to academia and industry, especially in the research and development communities."*
  - U.S. Attorney William Killian

Why Does the Government Control Exports?

Certain items and technologies are strategically important for:

- National Security Reasons
- Nuclear Non-Proliferation Reasons
- Missile Technology Controls
- Anti-Terrorism
- Chemical & Biological Controls
- Regional Stability
- Crime Control Measures
- Anti-boycott Reasons
- Economic Sanctions

Dual Use Technology: Export Control Considers Both

Technology that can be used for peaceful & military aims

Technology	Peaceful Use	Military Use
Carbon Fiber	Tennis Rackets	Ballistic Missile Nose Cones
Rocketry	Spaceflight	Missile Propulsion
GPS	Navigation	Guided Weapons Systems

Fermilab Dual Use Technology – Imaging Devices

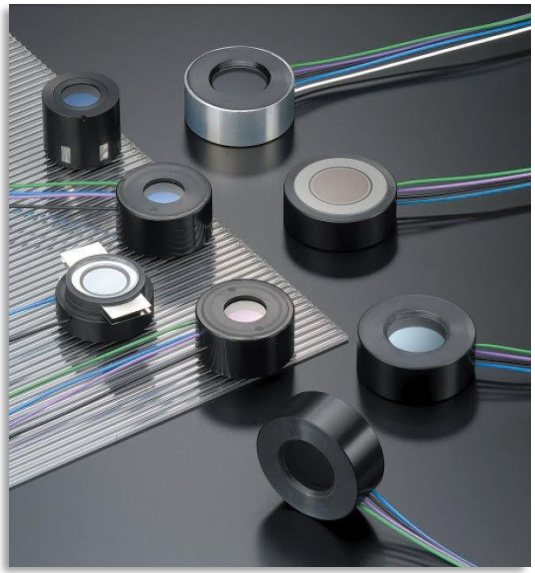
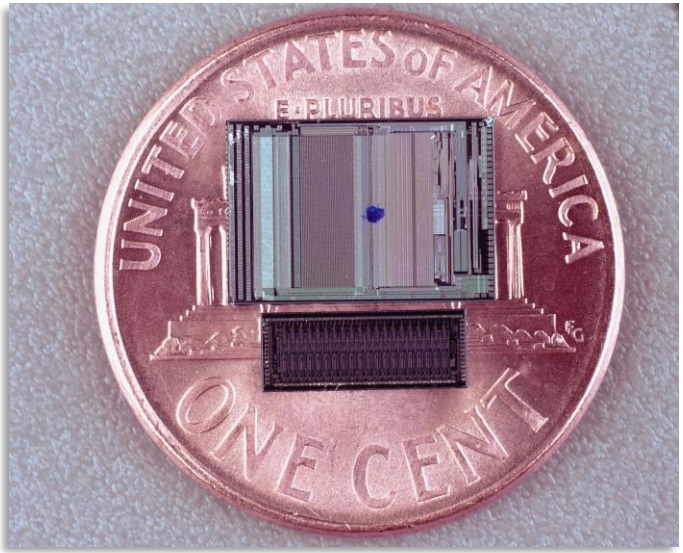


Image Intensifiers

Helmet Mounted Integrated Targeting

Patent Application # 62151535

Fermilab Dual Use Technology – Microchips



Particle Tracking

Electronic Warfare Countermeasure

Fundamental Research Exclusion (FRE)

- FRE excludes **technology** or **software** *resulting from*
  - Basic and applied research

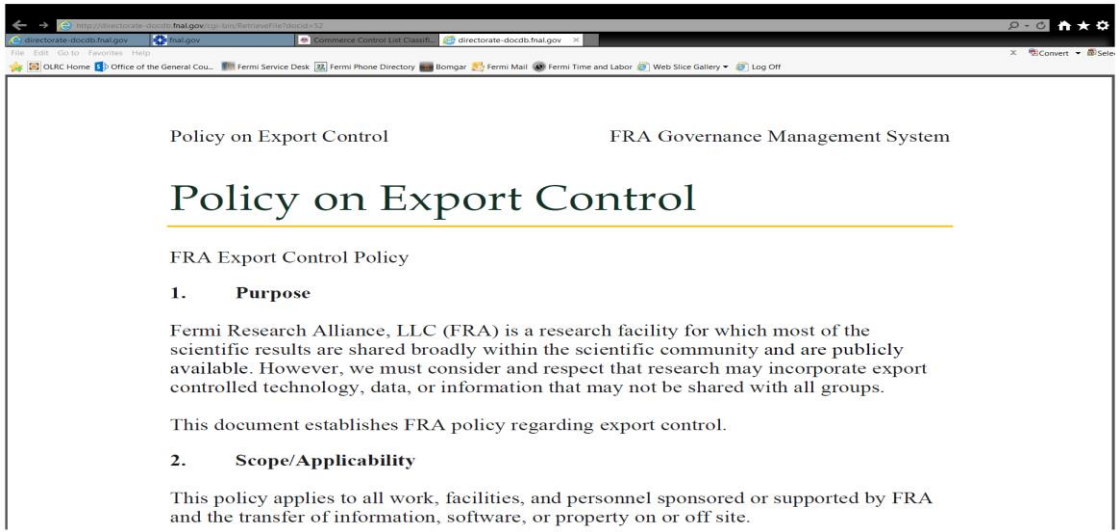
  In…
  - Science and engineering

  that is…
  - Ordinarily **published** and **shared** within scientific community

- **IMPORTANT:** Exclusion applies to information **output only**. **Technology, software and equipment used or accessed during research may be export controlled *even* if the results will be published.**
- Research restricted for national security reasons is ineligible.

Fermilab Export Control Policy

- Director's Policy – 12/31/16
- Strict adherence to Export Control laws, which applies to all work, facilities, and personnel. It also applies to transfers on or off site



Policy on Export Control FRA Governance Management System

Policy on Export Control

FRA Export Control Policy

1. Purpose

Fermi Research Alliance, LLC (FRA) is a research facility for which most of the scientific results are shared broadly within the scientific community and are publicly available. However, we must consider and respect that research may incorporate export controlled technology, data, or information that may not be shared with all groups.

This document establishes FRA policy regarding export control.

2. Scope/Applicability

This policy applies to all work, facilities, and personnel sponsored or supported by FRA and the transfer of information, software, or property on or off site.

Export Control Roles & Responsibilities

- Directorate – Ultimate responsibility for compliance
- Division/Section Heads/Managers/Project Leads/Hosts
  - Line management responsibility to engage process/compliance
- Office of General Counsel, Ex/Im Control Compliance Mgr.
  - Determination of export control status and licenses
- Logistics/Property Control Service
  - Proper export and import of items
- Office of Partnerships and Technology Transfer
  - Review of protected technologies
- WDRS
  - Immigration, visas, and international visits/users

Export Control Roles & Responsibilities (cont'd.)

- Procurement
  - Interface with suppliers/subcontractors
- Office of Communications
  - Tours and photos/videos at Lab
- All Employees
  - Support compliance
  - Engage the export control process and ask questions
  - Report possible ethics and compliance violations using the Fermilab Action Line (x4000)

Early engagement with Ex/Im Compliance Manager means better compliance and avoiding research delays

Applying Export Controls to Fermilab

- Research materials and technology may be export controlled
- Instruments may need restrictions on sharing within lab
- Licenses may be needed for foreign students/researchers/visitors participating on a project
- Licenses may be needed to bring items abroad for research
- Review of technical articles prior to publication

This does not mean that it is impossible for FRA to procure or ship an export-controlled item or that it is impossible for international users to participate. With **advance notice**, licenses or exceptions may be available for controlled items

Technical Publications & Ex/Im Compliance Review

Technical Publications (https://techpubs.fnal.gov/) **review applies to all scientific or technical materials intended for public release** (e.g., conference reports, physics notes, posters, publications, slides, technical memos, thesis, etc.):

- 1) Request a publication number: http://lss.fnal.gov/cgi-bin/getnumber.pl
- 2) Include acknowledgment, copyright info, and disclaimer
- 3) Upload
- 4) Tech Pubs & Ex/Im Comp review
- 5) External publication

- Thesis, then just 2 through 5

Export Control Review of Public Release of Information

- Submit information to Technical Publications for review **prior** to public release of information will reveal:
  - Specifications, code, or designs, or diagrams for building technical equipment
  - Instructions, manuals, or code for operating technical equipment
- Information of particular concern:
  - Nuclear-process simulation codes
  - Experiments or projects under proprietary or national security publication restricts
  - Emerging technology (e.g., AI, quantum computing, etc.)

Export Control Resources

Export/Import Control Compliance:

Paul Lauper Ellison (paule@fnal.gov or x3433)

Office of Partnerships & Technology Transfers:

Aaron Sauers (asauers@fnal.gov or x4432)

Global Services:

Griselda Lopez (griselda@fnal.gov or x6304)

Foreign Visits & Assignments:

Melissa Ormond (mormond@fnal.gov or x5061)

Ethics/Comp Hotline: *Fermilab Action Line (x4000)*

Cybersecurity is everyone's responsibility!

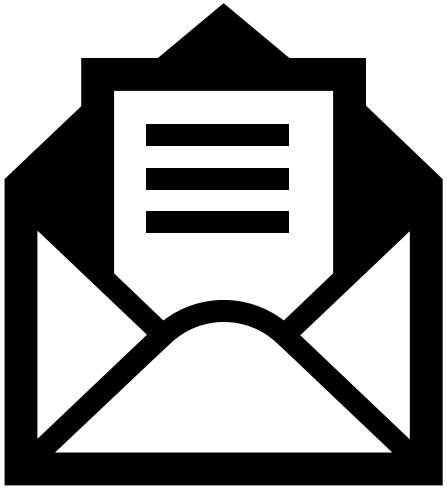
Why is cybersecurity training important?

- Fermilab is a government entity; all devices on the Fermilab network are tempting targets for attackers.
- A **single** individual's careless or unknowing action can cause significant harm to the entire laboratory.
- Cybersecurity is a partnership between the Cybersecurity Team (CST), lab management, users.
- As a Fermilab visitor, **YOU** are a user and a part of this partnership.
- **Your specific role:** accountable for the machines you have on the Fermi network.
- You must complete this training to obtain/renew your visitor badge.

Social engineering

- Social engineering is the process of tricking someone into disclosing personal information (such as username/password), or running malicious code on their computer.

- This is typically accomplished via **phishing emails** that are designed to look like real emails to lure you into clicking on a malicious link.



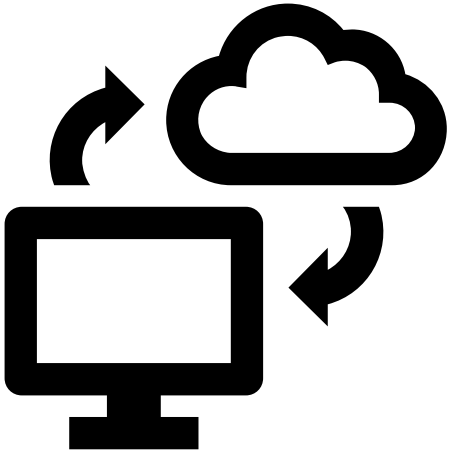
Signs of phishing emails to watch for:

- Emails that require immediate action or create a sense of urgency.
- Emails with generic salutations.
- Grammar or spelling mistakes.

Actions to take when you suspect phishing:

- Hover mouse over the links.
- Copy URLs from email to browser.
- Only open attachments you were expecting.
- Call and confirm if a friend/colleague sent the message.

Safe web browsing



- Web browsing is a primary contributor of malware. This occurs when legitimate websites have been compromised to redirect you to another site controlled by hackers.
- If you get a malware infection from visiting a site running malicious code, this is referred to as a **drive-by download.**

- **Practice safe web browsing habits with the following:**
  - Be careful when browsing!
  - Use an ad-blocker such as uBlock Origin.
  - **NEVER browse the web with an admin account.**
  - Only run up-to-date web browsers with up-to-date web components.
  - Run anti-virus with up-to-date virus signatures.

Physical security

- If an attacker gains physical access to your computer, it is effectively compromised because anything can be done to the machine at that point.

- **Maintaining physical security is easy:**
  - Always lock your screen when away from the computer.
    - Windows: Windows Key + L
    - Mac: Control + Command Q
  - Use a different password for every account, including SERVICES, FERMI, and Kerberos.
    More information: https://cd-docdb.fnal.gov/cgi-bin/sso/RetrieveFile?docid=3172&filename=AuthenticationPolicy.pdf&version=7
  - Do not leave unattended laptops in visible areas such as on a desk or in your car.
  - Machines in unlocked/common areas should use a cable lock to prevent theft.
  - Lock your office door at the end of the day if possible.

Policy highlights

- **Appropriate Use of Laboratory Computers and Fermilab Network**
  - Laboratory computers—or any devices on the laboratory network—should be used for laboratory business. Limited incidental use consistent with the Fermilab Policy on Computing on Prohibited Activities is allowed.
  - All computer users are required to behave in a way that maintains the security of the laboratory's computing environment.

- **Prohibited Use Of Laboratory Computers/Networks**
  - Illegal activities or activities that offend other employees or users or result in the embarrassment to the lab.
  - Uploading, downloading, viewing or storing sexually explicit material.
  - Uploading or downloading copyrighted material.
  - Using unlicensed software.
  - Activities in support of an ongoing private business.
  - Activities that consume excessive computing resources (disk space, network bandwidth, etc.).
  - Having unpatched or outdated devices on the network.
  - Bypassing Fermilab security controls.

-Reporting-

You must promptly report any actual, or even suspected, security breaches or incidents 24 x 7 to the Service Desk at x2345, or email the Cybersecurity Team at: cybersecurity@fnal.gov.

Detailed rules are provided in the Fermilab Policy on Computing.

Congratulations!

You have completed Basic Cybersecurity Training for Fermilab Visitors.

Please enter the following code on your Visitor Request Form to indicate that you have completed this training:

FermiCyber2019