

## Export Compliance Standard Operating Procedures (SOP)

Department:

Implementation Date:

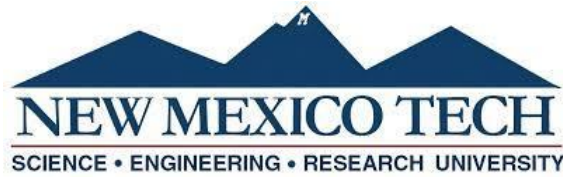
New Mexico Institute of Mining and Technology (NMT) is committed to full compliance with all applicable U.S. export control laws and regulations. As export controls continue to expand within the research environment, particularly with the rapid growth of artificial intelligence (AI) and advanced data-driven technologies, the University maintains the Export Compliance Program (ECP) and the Export Control Policy (OR-03.1-2025) to ensure appropriate oversight and to support faculty, staff, administrators, and students in understanding their compliance responsibilities.

The [Export Control Policy \(OR-03.1-2025\)](#) states the responsibility of all Academic, Research, and Administrative Units is to collaborate with the Export Control Officer (ECO) to:

- Develop procedures to manage compliance related to export controls
- Identify export control issues in relevant activities
- Provide guidance on international collaborations and travel

**Any questions or concerns regarding this SOP should be directed to:**

- New Mexico Tech Export Control Officer (ECO) -
  - Val Thomas - [export@npe.nmt.edu](mailto:export@npe.nmt.edu) or 575-835-5749
- New Mexico Tech Empowered Official (EO)
  - Dr. Carlos Romero - [carlos.romero@nmt.edu](mailto:carlos.romero@nmt.edu) or 505-554-7063



## Step 1 - CITI Training

NMT provides online export compliance training for all researchers, staff, and students involved in research through CITI. Individuals must complete the required initial training before beginning any project work and must participate in scheduled refresher training as directed by institutional procedures and the Export Control Officer (ECO). The ECO is responsible for tracking and maintaining all training records.

- NMT CITI Program Page:  
<https://www.nmt.edu/research/compliance/CITI%20Training.php>
  - Introduction to Export Compliance Module (ID 16800)

## Step 2 - Identify Potential Export Controlled Items

Use the following topics in conjunction with the NMT Export Compliance training, and The Bureau of Industry and Security's (BIS) [Guidance & Frequently Asked Questions](#) site to determine whether any equipment, data, software, or activity may fall under ITAR, EAR, or OFAC restrictions. This list is not exhaustive so it's always best to ask for an ECO review if you're unsure.

### 2.1 Identify What You're Using or Creating

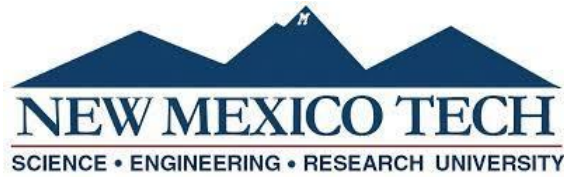
- Project items like equipment, software, prototypes, materials, technical data
- Project outputs like designs, models, code, datasets, schematics

### 2.2 Is the Information Public or Commonly Taught?

*Fundamental Research Exclusion (NSDD 189) This exclusion allows researchers to freely disseminate technical information without needing an export license, provided: there are no restrictions on publication or access (e.g., no sponsor-imposed limitations or citizenship-based access controls), and the research is not proprietary or tied to national security-sensitive development. The Office of Foreign Assets Control (OFAC) under the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security.*

- Published information (journals, websites, conferences)
- Standard coursework (appears in catalogs or syllabi)

If yes, it is **less likely** to be controlled.



### **2.3 Does It Have Military, Space, or Defense Use?**

- Defense applications like weapons, targeting, surveillance
- Space or missile systems
- Government restricted technology

If yes, *it may* fall under ITAR or sensitive EAR categories.

### **2.4 Could It Be Dual-Use?**

- Dual-use potential: civilian and military/security relevance
  - Examples: certain high-speed cameras, drones, lasers, advanced sensors, specialized materials or components

### **2.5 Does It Involve Encryption or Cybersecurity?**

*These often trigger EAR review and a Technology Control Plan (TCP).*

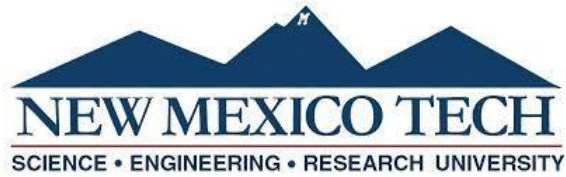
- Encryption software
- Secure communication tools
- Cryptographic development

### **2.6 Is Access or Publication Restricted?**

- Sponsor restrictions
- Confidential or proprietary data
- Non-public results
- Restrictions increase the likelihood of export control applicability.

### **2.7 Are Non US Persons Involved?**

- Foreign personnel
- International collaborators
- Foreign access to data or equipment
- Foreign access can trigger export control requirements even without physical export.



## **2.8 Will Anything Be Sent or Accessed Internationally?**

*These often trigger EAR review and a Technology Management Plan (TMP).*

- International shipments like materials, samples, equipment
- Digital transfers like cloud access, remote login
- Travel with equipment or data

## **2.9 Flag Any Uncertainty**

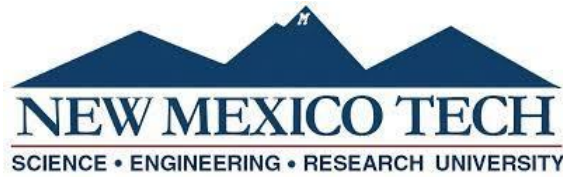
- Unclear classification
- Potential red flags
- When in doubt, escalate

## **2.10 Contact Research Compliance**

- Submit items for review
- Request classification help
- Provide brief notes on anything that triggered a “yes.”

If you have determined, based on the questions above that your project does not utilize items or information that is controlled, nothing further is required.

If you have determined, based on the questions above that an item or information is controlled, go to step 3.



### **Step 3 - Submit Export Control Information Form**

This form provides the ECO with the details needed to classify the item or activity.

- Complete the Export Control Information Form - [LINK](#)
  - *Please do not include any sensitive or controlled technical details in this form. Describe your project at a high level only. Do not upload designs, source code, schematics, or any information that may be export controlled.*

### **Step 4 - Receive Classification & Requirements**

Based on the form information the ECO determines regulatory classification and required controls and will reach out to you with.

- Review the assigned ECCN/USML category or OFAC determination
- Note any license requirements or Technology Control Plan (TCP) obligations
- Ask clarifying questions before proceeding

### **Step 5 - Implement Required Safeguards - Compliance Critical**

Apply physical, digital, and procedural controls based on the ECO's guidance.

- Restrict access to authorized personnel only
- Use approved storage, encryption, and access-control systems
- Maintain sign-in logs or digital access logs as required

### **Step 6 - Document All Actions Taken**

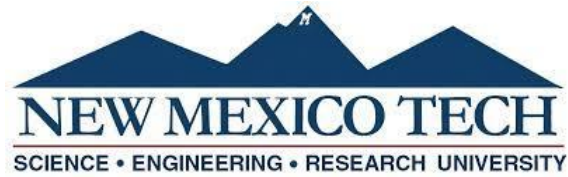
Maintain clear records demonstrating compliance throughout the project or activity.

- Save classification emails, TCPs, training records, and access logs
- Document any transfers, shipments, or foreign national interactions
- Retain records according to institutional retention schedules

### **Step 7 - Report Changes or Issues Immediately**

Notify the ECO of any deviations, new collaborators, equipment changes, or concerns.

- Report suspected violations or near-misses
- Request re-evaluation if project scope changes
- Do not proceed with new activities until cleared



## **Step 8 - Close Out and Archive**

Ensure all compliance obligations are met at the end of the activity.

- Return or secure controlled items
- Finalize documentation and submit required reports
- Confirm with the ECO that the project is formally closed