



UNLV

EXPORT CONTROL MANUAL



Table of Contents

Chapter 1 – Introduction.....	7
1.1 Purpose	7
1.2 Scope	7
1.3 Guiding Principles.....	8
1.4 Relationship to Research Security.....	9
1.5 Authority	9
Chapter 2 - Authority and Regulatory Framework	10
2.1 Federal Regulatory Authorities	10
2.2 Current Research Security Authorities	11
2.3 University Policy Framework.....	12
Chapter 3 - UNLV Export Control and Research Security Program	12
3.1 Program Objectives.....	12
3.2 Program Administration	12
3.3 Program Components.....	13
Chapter 4 - Roles and Responsibilities.....	15
4.1 Shared Responsibility	15
4.2 University President	15
4.3 Vice President for Research	15
4.4 Export Control Officer	15
4.5 Empowered Official	16
4.6 Principal Investigators.....	16
4.7 Department Chairs and Deans.....	16
4.8 Faculty and Staff.....	16
4.9 Students	17
Chapter 5- Export Control Fundamentals.....	17
5.1 What is an Export?	17
5.2 Deemed Exports	17
5.3 Export-Controlled Items	18
5.4 EAR99	18
5.5 Fundamental Research Exclusion	18
5.6 Publicly Available Information.....	19
5.7 Common University Activities Requiring Export Review	19

Chapter 6 - Export Administration Regulations (EAR)	20
6.1 Overview	20
6.2 Items Subject to the EAR	20
6.3 Export Control Classification Number (ECCN)	21
6.4 EAR99	22
6.5 License Determinations	22
6.6 Emerging Technologies	22
6.7 License Exceptions	23
Chapter 7 - International Traffic in Arms Regulations (ITAR).....	23
7.1 Overview	23
7.2 Defense Articles.....	23
7.3 Technical Data	24
7.4 Defense Services.....	24
7.5 United States Munitions List (USML).....	25
7.6 University Activities Subject to ITAR Review	25
7.7 Technology Control Plans	25
Chapter 8 - Office of Foreign Assets Control (OFAC)	26
8.1 Overview	26
8.2 Comprehensive and Targeted Sanctions	26
8.3 Specially Designated Nationals (SDN).....	26
8.4 Activities Requiring Review.....	27
8.5 OFAC Licenses.....	27
Chapter 9 - Other Federal Agency Export Controls.....	27
9.1 Additional Regulatory Authorities.....	27
9.2 Nuclear Technologies	28
9.3 Biological Materials	28
9.4 Controlled Chemicals.....	28
9.5 Controlled Software and Encryption	28
Chapter 10 - Research Security Requirements.....	29
10.1 Overview	29
10.2 National Security Presidential Memorandum-33 (NSPM-33)	29
10.3 Foreign Talent Recruitment Programs.....	29
10.4 International Collaborations	29

10.5 Cybersecurity and Controlled Research Data	30
10.6 Institutional Research Security Training	30
10.7 Reporting Concerns	31
Chapter 11 - Fundamental Research Exclusion (FRE).....	31
11.1 Purpose.....	31
11.2 Definition.....	31
11.3 Situations That May Eliminate the FRE	32
11.4 Sponsor Review.....	32
11.5 Principal Investigator Responsibilities.....	32
11.6 FRE Decision Checklist.....	32
Chapter 12 - Restricted Party Screening.....	33
12.1 Purpose.....	33
12.2 When Screening Is Required.....	33
12.3 Lists Reviewed.....	34
12.4 Positive Matches	34
12.5 Documentation.....	34
12.6 Screening Workflow	35
Chapter 13 - International Collaborations.....	35
13.1 Institutional Commitment.....	35
13.2 Activities Requiring Review	35
13.3 Collaboration Risk Assessment	35
13.4 Agreements	36
13.5 International Data Sharing	36
13.6 Best Practices	36
Chapter 14 - Foreign Visitors and International Scholars	37
14.1 Purpose.....	37
14.2 Activities Requiring Review	37
14.3 Visitor Review Process.....	37
14.4 Laboratory Access.....	37
14.5 Visiting Scholars	38
14.6 Documentation.....	38
Chapter 15 - International Travel.....	38
15.1 Overview	38

15.2 Activities Requiring Export Control Review	39
15.3 Temporary Exports.....	39
15.4 Sanctioned Countries	39
15.5 Data Security During Travel.....	39
15.6 Reporting	40
Chapter 16 - Shipping, Receiving, and International Transfers	40
16.1 Purpose.....	40
16.2 Activities Requiring Review	40
16.3 Shipping Review Process	41
16.4 Shipping Documentation	41
16.5 Hand-Carried Equipment	41
Chapter 17 - Technology Control Plans (TCPs).....	41
17.1 Purpose.....	41
17.2 When a TCP Is Required	41
17.3 Required Elements.....	42
17.4 Physical Security	42
17.5 Information Security	42
17.6 Training	43
Chapter 18 - Sponsored Research and Contract Review.....	43
18.1 Overview	43
18.2 Clauses Requiring Review.....	43
18.3 Proposal Stage Review	43
18.4 Award Acceptance	43
Chapter 19 - Procurement and Purchasing.....	44
19.1 Purpose.....	44
19.2 Purchases Requiring Review	44
19.3 Vendor Screening.....	44
19.4 Receiving Controlled Equipment.....	44
Chapter 20 - Information Security and Controlled Research Data	44
20.1 Overview	44
20.2 Controlled Information	44
20.3 Minimum Security Controls	45
20.4 Cloud Computing.....	45

20.5 Incident Reporting	45
Chapter 21 - Recordkeeping Requirements	45
21.1 Purpose.....	45
21.2 Records.....	45
21.3 Retention.....	46
Chapter 22 - Compliance Monitoring and Audits	46
22.1 Internal Reviews	46
22.2 Audits	46
22.3 Corrective Actions	46
Chapter 23 - Violations and Enforcement	46
23.1 Reporting Violations.....	46
23.2 Internal Investigation.....	46
23.3 Voluntary Self-Disclosure.....	47
23.4 Institutional Discipline	47
23.5 Federal Penalties.....	47
Chapter 24 – Definitions.....	47
Chapter 25 – Appendices	49

Chapter 1 – Introduction

1.1 Purpose

The University of Nevada, Las Vegas (UNLV) is committed to conducting research, education, public service, and innovation in a manner that complies with all applicable United States export control laws, economic sanctions regulations, and federal research security requirements.

The purpose of this Manual is to establish the University's Export Control and Research Security Program by providing guidance for faculty, staff, students, visiting scholars, and affiliates whose activities may involve:

- International research collaborations
- International travel
- International shipping
- Foreign national participation in research
- Controlled technology
- Export-controlled equipment
- Biological materials
- Software and encryption
- Sponsored research
- Procurement
- International financial transactions

This Manual establishes institutional procedures designed to:

- Protect national security interests
- Support compliance with federal law
- Preserve academic freedom whenever possible
- Facilitate international research responsibly
- Reduce institutional risk
- Promote responsible stewardship of sponsored research

1.2 Scope

This Manual applies to all UNLV colleges, schools, departments, centers, institutes, laboratories, administrative units, affiliated organizations, and all individuals conducting activities on behalf of the University, including:

- Faculty
- Staff
- Students
- Visiting scientists
- Postdoctoral scholars
- Volunteers
- Emeritus faculty
- Contractors
- Consultants
- Affiliates

The requirements contained herein apply regardless of funding source and include:

- Federally sponsored research
- State-funded activities
- Industry-sponsored research
- Clinical research
- International partnerships
- Educational activities
- Service agreements
- Procurement
- Technology commercialization

1.3 Guiding Principles

UNLV recognizes that:

Academic openness is fundamental to research excellence.

At the same time, the University must safeguard technologies, information, and activities that are regulated by the U.S. Government.

Accordingly, UNLV seeks to:

- Encourage international collaboration
- Protect controlled technologies
- Maintain compliance with export regulations

- Promote ethical research practices
- Protect national security
- Support responsible innovation

Compliance with export control regulations is a shared institutional responsibility.

1.4 Relationship to Research Security

Export control compliance is one component of the University's broader Research Security Program.

Research security encompasses:

- Export Controls
- Foreign Influence
- Research Integrity
- Cybersecurity
- Controlled Unclassified Information (CUI)
- Sensitive Research Security
- Foreign Talent Recruitment Program compliance
- International collaboration risk management

Together, these activities protect:

- Research personnel
 - Sensitive technology
 - Intellectual property
 - Federal funding
 - National security
-

1.5 Authority

This Manual supports implementation of:

- NSHE Chapter 14 Export Control and Economic Sanctions Policy
- UNLV Research Integrity policies
- UNLV Information Security policies
- Federal sponsor requirements
- Applicable U.S. laws and regulations

Chapter 2 - Authority and Regulatory Framework

2.1 Federal Regulatory Authorities

Export controls are administered by multiple federal agencies.

Department of Commerce

Bureau of Industry and Security (BIS)

Regulations:

Export Administration Regulations (EAR)

15 CFR Parts 730–774

Responsible for regulating:

- Dual-use technology
- Commercial items
- Emerging technologies
- Advanced computing
- Semiconductor technology
- Encryption
- Certain military items

Department of State

Directorate of Defense Trade Controls (DDTC)

Regulations:

International Traffic in Arms Regulations (ITAR)

22 CFR Parts 120–130

Responsible for regulating:

- Defense articles
- Defense services
- Technical data
- Space technologies
- Military systems

Department of the Treasury

Office of Foreign Assets Control (OFAC)

Regulations:

31 CFR Chapter V

Responsible for:

- Economic sanctions
- Embargoes
- Blocked persons
- Financial restrictions
- Country sanctions

Additional Agencies

Activities conducted at UNLV may also be subject to regulations administered by:

- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)
- National Science Foundation (NSF)
- National Institute of Health (NIH)
- Department of Defense (DOD)
- National Aeronautics and Space Administration (NASA)
- Food and Drug Administration (FDA)
- Drug Enforcement Administration (DEA)
- Others

2.2 Current Research Security Authorities

UNLV's compliance program incorporates applicable federal research security expectations, including:

- National Security Presidential Memorandum-33 (NSPM-33)
- CHIPS and Science Act
- OSTP Research Security Guidelines

- NSF Research Security Requirements
 - NIH Foreign Subrecipient and Disclosure Requirements
 - DOE Order 486.1 (when applicable)
 - DoD Research Security policies
 - NASA Research Security guidance
-

2.3 University Policy Framework

Institutional authority is derived from:

- NSHE Procedures and Guidelines Manual Chapter 14
 - UNLV institutional policies
 - Sponsored Projects Administration procedures
 - Office of Research Integrity procedures
 - Information Security Program
 - Applicable federal award terms and conditions
-

Chapter 3 - UNLV Export Control and Research Security Program

3.1 Program Objectives

The Export Control Program is designed to:

- Ensure compliance with U.S. export laws
 - Support international research
 - Protect controlled technology
 - Facilitate responsible collaboration
 - Reduce institutional risk
 - Protect federal funding
-

3.2 Program Administration

The program is administered through the Office of Research Integrity under the authority delegated by the Vice President for Research.

The University President designates:

- Export Control Officer (ECO)

- Empowered Official (EO)

These officials are authorized to:

- Classify technologies
 - Conduct export reviews
 - Submit export license applications
 - Develop Technology Control Plans
 - Conduct Restricted Party Screening
 - Provide institutional guidance
 - Coordinate federal agency communications
-

3.3 Program Components

The UNLV Export Control Program includes:

Export Reviews

Review of:

- Research proposals
 - Contracts
 - Material Transfer Agreements
 - NDAs
 - Equipment purchases
 - International collaborations
-

Restricted Party Screening

Screening includes:

- Individuals
- Universities
- Companies
- Sponsors
- Visitors
- Vendors

- Collaborators
 - Shipping recipients
-

Technology Classification

Including:

- ECCN determinations
 - ITAR jurisdiction
 - EAR99 determinations
 - License reviews
-

Licensing

Preparation and submission of:

- BIS licenses
 - DDTC licenses
 - OFAC licenses
-

Technology Control Plans

Development and monitoring of project-specific TCPs.

Education

The University provides:

- Faculty training
 - PI workshops
 - Online resources
 - Individual consultations
-

Compliance Monitoring

Including:

- Internal reviews
- Audits

- Corrective actions
 - Recordkeeping
-

Chapter 4 - Roles and Responsibilities

4.1 Shared Responsibility

Compliance with export control regulations is the responsibility of every member of the University community.

4.2 University President

The President shall:

- Support institutional compliance
 - Designate the Empowered Official
 - Ensure adequate institutional resources
-

4.3 Vice President for Research

Responsible for:

- Oversight of institutional compliance
 - Allocation of program resources
 - Research security governance
-

4.4 Export Control Officer

The Export Control Officer shall:

- Administer the Export Control Program
- Conduct export reviews
- Determine regulatory jurisdiction
- Coordinate licensing
- Conduct Restricted Party Screening
- Develop Technology Control Plans
- Deliver training
- Maintain records

- Conduct investigations
 - Coordinate with federal agencies
-

4.5 Empowered Official

The Empowered Official possesses authority to:

- Sign export license applications
 - Certify institutional compliance
 - Bind the University before federal agencies
 - Stop activities presenting unacceptable export risks
-

4.6 Principal Investigators

Principal Investigators are responsible for:

- Consulting the ECO early
 - Identifying export-controlled research
 - Reporting foreign collaborations
 - Protecting controlled technology
 - Completing required training
 - Following Technology Control Plans
 - Reporting potential violations immediately
-

4.7 Department Chairs and Deans

Responsible for:

- Supporting compliance
 - Promoting faculty awareness
 - Ensuring departmental cooperation
 - Supporting corrective actions
-

4.8 Faculty and Staff

Responsible for:

- Completing required training
- Consulting the ECO

- Following approved procedures
 - Reporting concerns promptly
-

4.9 Students

Students participating in research shall:

- Follow Technology Control Plans
 - Protect controlled information
 - Complete required training
 - Report concerns
-

Chapter 5- Export Control Fundamentals

5.1 What is an Export?

An export includes more than shipping items overseas.

An export may occur through:

- Shipping equipment
 - Emailing technical data
 - Cloud file sharing
 - Remote access
 - Oral discussions
 - Laboratory demonstrations
 - Visual inspections
 - Software downloads
 - Hand carrying equipment abroad
-

5.2 Deemed Exports

A deemed export occurs when controlled technology is released to a foreign person within the United States.

Examples include:

- Laboratory instruction
- Sharing engineering drawings

- Software demonstrations
 - Research meetings
 - Access to controlled databases
-

5.3 Export-Controlled Items

Examples include:

- Lasers
 - UAV technology
 - Satellite components
 - Thermal imaging
 - Navigation systems
 - High-performance computing equipment
 - Encryption software
 - Controlled biological agents
 - Specialized sensors
-

5.4 EAR99

Many commercial items exported by universities are designated EAR99.

Although generally low risk, EAR99 items may still require authorization when exported:

- To sanctioned countries
 - To prohibited end users
 - For prohibited end uses
 - In support of weapons proliferation
-

5.5 Fundamental Research Exclusion

Most university research qualifies as Fundamental Research under federal regulations.

Research generally qualifies when:

- Results are ordinarily published
- Participation is unrestricted
- No publication restrictions are accepted

- No citizenship restrictions are imposed

The exclusion generally does **not** apply when:

- Sponsors restrict publication beyond limited review for proprietary information or patent protection.
- Sponsors restrict participation based on citizenship or nationality.
- Research involves controlled technical data provided by a sponsor under confidentiality obligations.
- The activity involves defense services, controlled equipment, or exports of tangible items.

Investigators should consult the Export Control Officer before accepting contractual provisions that may limit publication, dissemination, or participant eligibility, as such terms may eliminate the availability of the Fundamental Research Exclusion.

5.6 Publicly Available Information

Information that is lawfully published and generally accessible to the public is ordinarily outside the scope of export controls.

Examples include:

- Published journal articles
- Public conference presentations
- Publicly available patents
- Information released without restriction
- University catalog course materials
- Public websites

5.7 Common University Activities Requiring Export Review

Activities that frequently require consultation with the Export Control Officer include:

Activity	Review Recommended
International shipment of equipment	✓
Hiring foreign researchers for controlled projects	✓
International collaborations	✓
Military sponsor	✓

Activity	Review Recommended
Encryption software	✓
International travel with research equipment	✓
Sponsored agreements with publication restrictions	✓
Material Transfer Agreements	✓
Visiting scholars accessing controlled laboratories	✓

Chapter 6 - Export Administration Regulations (EAR)

6.1 Overview

The Export Administration Regulations (EAR), administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), regulate the export, re-export, and transfer (in-country) of commercial, dual-use, and certain military items that do not fall under the jurisdiction of the International Traffic in Arms Regulations (ITAR).

The EAR applies to:

- Commodities
- Equipment
- Software
- Technology
- Technical information
- Source code
- Certain services
- Emerging and foundational technologies

Unlike ITAR, which generally controls defense articles, the EAR governs a much broader range of items encountered in university research.

6.2 Items Subject to the EAR

Items subject to the EAR generally include:

- Scientific instrumentation
- High-performance computers

- Semiconductor equipment
- Artificial intelligence technologies
- Quantum information systems
- Lasers
- Sensors
- Drones (certain models)
- Telecommunications equipment
- Navigation systems
- Encryption software
- Biotechnology equipment

6.3 Export Control Classification Number (ECCN)

Most controlled items regulated under the EAR are assigned an Export Control Classification Number (ECCN).

Each ECCN identifies:

- Technical characteristics
- Reasons for control
- Licensing requirements
- Applicable license exceptions

The Commerce Control List (CCL), Supplement No. 1 to Part 774 of the EAR, organizes ECCNs into ten categories and five product groups.

CCL Categories

Category Description

0	Nuclear Materials, Facilities, and Miscellaneous
1	Materials, Chemicals, Microorganisms, and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Telecommunications and Information Security

Category Description

6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

6.4 EAR99

Items not specifically identified on the CCL are generally designated EAR99.

EAR99 items typically do not require an export license unless:

- Exported to sanctioned destinations
- Exported to prohibited parties
- Intended for prohibited end uses
- Associated with weapons proliferation activities

Even routine laboratory equipment may require review before international shipment.

6.5 License Determinations

The Export Control Officer determines whether a BIS export license is required by evaluating:

- ECCN
- Country of destination
- End user
- End use
- Applicable license exceptions

No University employee may independently determine that an export license is unnecessary without consultation with the Export Control Officer when uncertainty exists.

6.6 Emerging Technologies

Federal regulations continue to evolve regarding:

- Artificial Intelligence
- Advanced computing
- Semiconductor manufacturing

- Quantum computing
- Advanced biotechnology
- Hypersonic technologies
- Additive manufacturing

Researchers working in these areas should consult the Export Control Officer during proposal development.

6.7 License Exceptions

Certain exports may qualify for EAR License Exceptions, including:

- TMP (Temporary Exports)
- BAG (Personal Baggage)
- GOV (Government)
- ENC (Encryption Commodities, Software, and Technology)
- TSU (Technology and Software—Unrestricted)

Only the Export Control Officer may authorize institutional reliance on a License Exception.

Chapter 7 - International Traffic in Arms Regulations (ITAR)

7.1 Overview

The International Traffic in Arms Regulations (ITAR), administered by the U.S. Department of State Directorate of Defense Trade Controls (DDTC), regulate defense articles, defense services, and related technical data.

ITAR protects technologies directly related to national defense and military capability.

7.2 Defense Articles

Defense articles include items specifically designed, developed, configured, adapted, or modified for military applications and listed on the United States Munitions List (USML).

Examples include:

- Military aircraft
- Missile components
- Weapons systems
- Night vision devices

- Military electronics
 - Space-related defense technologies
 - Fire control systems
-

7.3 Technical Data

Technical data includes information required for:

- Design
- Development
- Production
- Assembly
- Testing
- Repair
- Maintenance
- Modification

Technical data may exist in:

- CAD files
 - Engineering drawings
 - Software
 - Emails
 - Laboratory notebooks
 - Photographs
 - Oral discussions
-

7.4 Defense Services

Defense services include:

- Training
- Technical assistance
- Consulting
- Instruction
- Design support

- Troubleshooting
- Integration of defense articles

Providing assistance to a foreign person regarding an ITAR-controlled defense article may require prior DDTC authorization.

7.5 United States Munitions List (USML)

The USML consists of twenty-one categories of controlled defense articles.

The Export Control Officer shall determine whether equipment, software, or technical data falls within USML jurisdiction.

7.6 University Activities Subject to ITAR Review

Examples include:

- Defense-sponsored research
 - Military prototypes
 - Space systems
 - Satellite components
 - Defense contracts
 - Military vehicle testing
 - Certain UAV research
 - Controlled defense software
-

7.7 Technology Control Plans

Projects involving ITAR-controlled information require a Technology Control Plan before project activities begin.

TCPs may include:

- Controlled laboratory access
- Visitor restrictions
- Secure information technology
- Locked storage
- Personnel training
- Citizenship verification where legally permissible
- Recordkeeping requirements

Chapter 8 - Office of Foreign Assets Control (OFAC)

8.1 Overview

The Office of Foreign Assets Control (OFAC), U.S. Department of the Treasury, administers economic sanctions and embargo programs designed to protect U.S. foreign policy and national security interests.

OFAC regulations may prohibit:

- Financial transactions
- Research collaborations
- Services
- Travel-related activities
- Imports
- Exports

8.2 Comprehensive and Targeted Sanctions

OFAC administers both:

- Comprehensive country sanctions
- Targeted sanctions directed at individuals, entities, organizations, or specific sectors

Sanctions programs change frequently and must be reviewed before international activities.

8.3 Specially Designated Nationals (SDN)

The SDN List identifies persons and organizations with whom U.S. persons are generally prohibited from conducting business.

Prior to engaging in international activities, the University screens:

- Collaborators
- Vendors
- Sponsors
- Visitors
- Students (where appropriate)
- Shipping recipients

- Foreign institutions
-

8.4 Activities Requiring Review

Consult the Export Control Officer before:

- Conducting research in sanctioned countries
 - Paying foreign collaborators
 - Shipping equipment internationally
 - Hosting sanctioned entities
 - International consulting
 - Providing online instruction involving sanctioned jurisdictions
 - Conducting field research abroad
-

8.5 OFAC Licenses

Certain activities may be authorized through:

- General Licenses
- Specific Licenses

Only the Export Control Officer, in coordination with the Empowered Official where appropriate, may coordinate institutional license requests.

Chapter 9 - Other Federal Agency Export Controls

9.1 Additional Regulatory Authorities

Certain University activities are regulated by agencies beyond BIS, DDTC, and OFAC.

Examples include:

- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)
- National Nuclear Security Administration (NNSA)
- Department of Agriculture (USDA)
- Food and Drug Administration (FDA)
- Drug Enforcement Administration (DEA)
- Environmental Protection Agency (EPA)

9.2 Nuclear Technologies

Research involving:

- Nuclear materials
- Nuclear reactors
- Radiation technologies
- Sensitive nuclear information

may require additional federal authorization.

9.3 Biological Materials

Controlled biological materials include:

- Select agents
- Certain toxins
- Dangerous pathogens
- Genetically modified organisms subject to federal regulation

Research involving these materials should be coordinated with Environmental Health and Safety, the Institutional Biosafety Committee, and the Export Control Officer.

9.4 Controlled Chemicals

Certain chemicals may require additional review due to:

- Chemical Weapons Convention regulations
 - Commerce controls
 - Environmental regulations
 - DEA requirements
-

9.5 Controlled Software and Encryption

Software involving:

- Strong encryption
- Secure communications
- Network security
- Artificial intelligence applications

- Cybersecurity tools

may be regulated under the EAR and should be evaluated prior to international distribution.

Chapter 10 - Research Security Requirements

10.1 Overview

Federal research sponsors increasingly require institutions to maintain comprehensive research security programs that protect the integrity, security, and openness of federally funded research.

UNLV's Research Security Program complements its Export Control Program and supports compliance with sponsor requirements while preserving academic freedom and international collaboration.

10.2 National Security Presidential Memorandum-33 (NSPM-33)

UNLV shall implement institutional processes consistent with NSPM-33 and applicable federal agency guidance, including measures related to:

- Research security program administration
- Disclosure of outside professional activities and appointments
- Disclosure of foreign affiliations and support
- Research security training
- Cybersecurity practices, as applicable to sponsored research
- Protection of federally funded research and associated information

Investigators are responsible for providing complete, accurate, and timely disclosures required by sponsors and the University.

10.3 Foreign Talent Recruitment Programs

Certain foreign talent recruitment programs are prohibited under federal law and sponsor requirements.

Faculty, staff, and researchers must consult the Office of Research Integrity before participating in any foreign recruitment, appointment, or similar program that could implicate federal restrictions.

10.4 International Collaborations

International collaborations are encouraged when conducted in accordance with applicable laws and sponsor requirements.

Prior to initiating high-risk international collaborations, investigators should coordinate with the Export Control Officer to assess:

- Export control implications
 - Research security considerations
 - Restricted party status
 - Contractual obligations
 - Data protection requirements
 - Sponsor-specific conditions
-

10.5 Cybersecurity and Controlled Research Data

Research involving export-controlled information, Controlled Unclassified Information (CUI), or sponsor-designated sensitive information shall employ security controls appropriate to the applicable legal, regulatory, contractual, and institutional requirements.

Such controls may include:

- Multi-factor authentication
- Encryption of data at rest and in transit
- Access controls based on authorized need
- Secure storage and transmission
- Logging and monitoring where appropriate
- Incident reporting procedures

The University Information Security Office and the Export Control Officer should be consulted when projects involve controlled or sensitive research information.

10.6 Institutional Research Security Training

Individuals whose responsibilities involve export-controlled research, international activities, or other research security risks shall complete required institutional training before engaging in covered activities and thereafter as required by University policy or sponsor requirements.

Training topics may include:

- Export controls
- Research security
- Foreign influence awareness
- International travel

- Cybersecurity
 - Data protection
 - Responsible international collaboration
-

10.7 Reporting Concerns

Members of the University community are expected to promptly report suspected export control or research security concerns to the Export Control Officer or the Office of Research Integrity.

The University will review reported concerns, implement appropriate corrective actions, and, when required, make notifications to sponsoring agencies or federal authorities in accordance with applicable laws, regulations, award terms, and institutional policy.

Chapter 11 - Fundamental Research Exclusion (FRE)

11.1 Purpose

The Fundamental Research Exclusion (FRE) is one of the most important exclusions available to universities conducting scientific research. Proper application of the FRE allows the results of qualifying research to be shared openly without being subject to export licensing requirements for the dissemination of resulting information.

The FRE does **not** exempt:

- Tangible exports (equipment, materials, prototypes)
- Controlled software
- ITAR defense articles
- Transactions prohibited by OFAC
- Controlled technical data received from third parties

Investigators should not assume that an entire project is exempt simply because it occurs at a university.

11.2 Definition

Fundamental research is basic or applied research in science or engineering for which the resulting information is ordinarily published and shared broadly within the scientific community.

Research generally qualifies when:

- Results are intended for publication.
- Researchers are free to discuss findings openly.

- There are no unreasonable publication restrictions.
- Participation is not restricted based on citizenship or nationality.

11.3 Situations That May Eliminate the FRE

The exclusion may no longer apply if UNLV accepts contractual terms that:

- Restrict publication beyond limited review for proprietary information or patent protection.
- Restrict participation by foreign nationals.
- Require sponsor approval before publication.
- Limit dissemination of research results.
- Require access restrictions inconsistent with open research.

Acceptance of these provisions should be reviewed by the Export Control Officer (ECO) during contract negotiation.

11.4 Sponsor Review

Limited sponsor review for the following purposes generally does **not** invalidate the FRE:

- Protection of proprietary information
 - Patent filings
 - Removal of confidential sponsor information
-

11.5 Principal Investigator Responsibilities

Principal Investigators shall:

- Notify the ECO of any publication restrictions.
 - Avoid accepting unauthorized access restrictions.
 - Consult the ECO before agreeing to export control clauses.
 - Report changes in project scope that may affect the applicability of the FRE.
-

11.6 FRE Decision Checklist

Investigators should consider the following questions:

Question	Yes	No
Is the research intended for publication?	☐	☐

Question	Yes	No
Are foreign nationals permitted to participate?	☐	☐
Does the agreement avoid publication approval requirements?	☐	☐
Is the research free from dissemination restrictions?	☐	☐

If any answer is **No**, the investigator should consult the Export Control Officer.

Chapter 12 - Restricted Party Screening

12.1 Purpose

Federal regulations prohibit UNLV from engaging in certain activities involving restricted individuals, organizations, and governments. Restricted Party Screening (RPS) helps ensure that the University does not knowingly conduct prohibited transactions.

12.2 When Screening Is Required

Restricted Party Screening should be conducted before:

- Entering sponsored research agreements
- Executing subawards
- International shipments
- Purchasing from foreign vendors
- International consulting
- International collaborations
- Hosting visiting scholars
- Executing Material Transfer Agreements
- Technology licensing
- International travel involving institutional business
- International financial transactions

Additional screening should occur whenever new parties are added to an activity or when the nature of the engagement changes.

12.3 Lists Reviewed

The University's screening process may include review of applicable federal restricted party lists, including:

- BIS Entity List
 - BIS Denied Persons List
 - BIS Unverified List
 - OFAC Specially Designated Nationals (SDN) List
 - DDTC Debarred Parties List
 - DOD 1286 List or DOD 1260(H) List
 - Other applicable U.S. government restricted party lists
-

12.4 Positive Matches

Potential matches shall be reviewed by the Export Control Officer.

University personnel shall not independently determine whether a potential match is acceptable.

If a confirmed restricted party is identified:

- Activities shall be paused.
 - The Export Control Officer shall evaluate the transaction.
 - Licenses or other authorizations will be obtained when legally available and appropriate.
 - Activities prohibited by law shall not proceed.
-

12.5 Documentation

The Export Control Office shall maintain records of:

- Screening date
- Parties screened
- Databases used
- Screening results
- Follow-up actions
- Licensing determinations, if applicable

Records shall be retained in accordance with institutional record retention requirements and applicable federal regulations.

12.6 Screening Workflow

1. Identify all parties.
 2. Conduct restricted party screening.
 3. Review any potential matches.
 4. Determine whether additional review or licensing is required.
 5. Document the outcome.
 6. Proceed only after approval, if required.
-

Chapter 13 - International Collaborations

13.1 Institutional Commitment

UNLV values international research collaborations and recognizes that global engagement advances discovery, innovation, and education. International partnerships should be conducted in a manner that protects research integrity and complies with export control, sanctions, sponsor, and research security requirements.

13.2 Activities Requiring Review

The Export Control Officer should be consulted before initiating collaborations that involve:

- Foreign governments
 - Foreign military organizations
 - Export-controlled technology
 - Controlled biological materials
 - Defense-related research
 - International laboratories
 - Sensitive technologies
 - Sponsored research with foreign entities
-

13.3 Collaboration Risk Assessment

Factors considered during review may include:

- Country risk
- Export-controlled technology
- Research sponsor requirements

- Data security needs
- Restricted party status
- Intellectual property considerations
- Funding source
- Nature of the research activity

The level of institutional review should be proportionate to the identified risks.

13.4 Agreements

The Export Control Office should coordinate with Sponsored Programs and the Office of General Counsel, as appropriate, when reviewing agreements that may include:

- Publication restrictions
 - Confidentiality obligations
 - Technology transfer provisions
 - Intellectual property clauses
 - Export control clauses
 - Foreign government participation
-

13.5 International Data Sharing

Researchers should consult the Export Control Officer and Information Security Office before transferring controlled or sensitive research information internationally.

Considerations include:

- Export-controlled technical data
 - Controlled Unclassified Information (CUI)
 - Personally identifiable information
 - Human subject data
 - Encryption requirements
 - Sponsor-imposed restrictions
-

13.6 Best Practices

Researchers are encouraged to:

- Engage the Export Control Office early.

- Clearly define project scope.
 - Maintain appropriate documentation.
 - Use secure University-approved systems for data storage and sharing.
 - Comply with sponsor disclosure requirements.
-

Chapter 14 - Foreign Visitors and International Scholars

14.1 Purpose

UNLV welcomes international visitors and scholars as an essential part of its academic mission. Appropriate planning helps ensure that these activities are conducted in compliance with export control and research security requirements.

14.2 Activities Requiring Review

Review by the Export Control Officer may be appropriate when visitors will:

- Access export-controlled laboratories
 - Receive controlled technical data
 - Observe controlled equipment
 - Participate in defense-related research
 - Access sponsor-restricted information
 - Visit secured research facilities
-

14.3 Visitor Review Process

The review process may include:

- Identification of the visitor and sponsoring department
 - Assessment of the proposed activities
 - Restricted Party Screening
 - Evaluation of applicable export control requirements
 - Determination of whether a Technology Control Plan is required
-

14.4 Laboratory Access

Where controlled research is conducted, access may be limited to authorized personnel in accordance with project requirements and applicable law.

Protective measures may include:

- Escort requirements
 - Badge restrictions
 - Visitor logs
 - Controlled access areas
 - Secure storage of controlled materials and information
-

14.5 Visiting Scholars

Departments hosting visiting scholars should coordinate with the Export Control Office when activities involve:

- Sensitive technologies
 - Sponsored research restrictions
 - Controlled equipment
 - International shipping
 - Access to controlled technical information
-

14.6 Documentation

Departments should maintain appropriate documentation regarding:

- Visitor purpose
 - Dates of visit
 - Host department
 - Screening, when required
 - Applicable approvals
-

Chapter 15 - International Travel

15.1 Overview

International travel conducted on behalf of UNLV may implicate export control, sanctions, customs, sponsor, and research security requirements. Advance planning helps reduce risk and ensures compliance.

15.2 Activities Requiring Export Control Review

Travelers should consult the Export Control Officer before traveling internationally with:

- University-owned laptops
- Specialized research equipment
- Controlled software
- Encryption technology
- Biological materials
- Research samples
- Laboratory instruments
- Drones
- Prototype devices

Review is also recommended when travel involves sanctioned jurisdictions or restricted entities.

15.3 Temporary Exports

Many temporary exports of University equipment may qualify for a license exception or other authorization under applicable regulations; however, eligibility depends on the specific facts.

Travelers should not assume that carrying equipment abroad is exempt from export control requirements.

15.4 Sanctioned Countries

Travel involving countries subject to comprehensive or significant U.S. sanctions may require additional institutional review or federal authorization.

Travelers should consult the Export Control Office well in advance of departure when travel involves sanctioned jurisdictions.

15.5 Data Security During Travel

International travelers should:

- Use University-approved devices whenever practicable.
- Enable multi-factor authentication.
- Use encrypted storage where appropriate.
- Avoid storing unnecessary sensitive data on travel devices.
- Connect through secure networks and approved virtual private network (VPN) services when available.

- Report loss or compromise of University devices promptly.

Travel involving export-controlled or sponsor-restricted information may require additional security measures coordinated with the Information Security Office.

15.6 Reporting

Upon return, travelers should promptly report to the Export Control Officer any:

- Customs issues
- Unexpected requests for technical information
- Device inspections that may have involved access to University information
- Lost or stolen equipment
- Potential export control or sanctions concerns encountered during travel

Chapter 16 - Shipping, Receiving, and International Transfers

16.1 Purpose

The shipment, transfer, hand-carry, or electronic transmission of items, software, biological materials, and technical information outside the United States may constitute an export under U.S. law. UNLV personnel must coordinate international transfers with the Export Control Officer (ECO) to ensure compliance with applicable regulations.

16.2 Activities Requiring Review

The ECO should review international transfers involving:

- Research equipment
- Scientific instruments
- Biological materials
- Chemicals
- Radioactive materials
- Prototype devices
- Laboratory samples
- Encryption software
- Technical data
- Controlled software
- Defense articles
- Research specimens

16.3 Shipping Review Process

Prior to shipment:

1. Determine item classification (EAR99, ECCN, or USML).
2. Screen all parties.
3. Determine destination country restrictions.
4. Evaluate end use and end user.
5. Determine licensing requirements.
6. Obtain federal authorization if required.
7. Maintain export documentation.

16.4 Shipping Documentation

Required documentation may include:

- Commercial invoices
- Packing lists
- Air waybills
- Export declarations
- License documentation
- Material Transfer Agreements
- Customs paperwork

16.5 Hand-Carried Equipment

Faculty traveling internationally with research equipment should consult the ECO before departure.

Chapter 17 - Technology Control Plans (TCPs)

17.1 Purpose

A Technology Control Plan (TCP) establishes administrative, physical, and information security measures that prevent unauthorized access to export-controlled items, software, and technical data.

17.2 When a TCP Is Required

A TCP may be required when:

- ITAR-controlled information is involved.
- Controlled technical data is received.

- A sponsored agreement restricts access.
- Export-controlled equipment is used.
- A federal license requires access controls.

17.3 Required Elements

Each TCP should identify:

- Project description
- Controlled technologies
- Responsible personnel
- Authorized project members
- Physical security
- Information security
- Visitor procedures
- Training requirements
- Recordkeeping
- Project closeout procedures

17.4 Physical Security

Examples include:

- Card-access laboratories
- Locked offices
- Locked cabinets
- Visitor escort requirements
- Equipment inventories

17.5 Information Security

Examples include:

- Multi-factor authentication
- Encryption
- Network segmentation
- Access logging
- Secure backups
- Password management

17.6 Training

All personnel covered by a TCP shall receive documented training before receiving access.

Chapter 18 - Sponsored Research and Contract Review

18.1 Overview

Sponsored research agreements frequently contain provisions affecting export control compliance.

The ECO shall coordinate with the Office of Sponsored Programs during contract review when export control concerns are identified.

18.2 Clauses Requiring Review

Examples include:

- Publication restrictions
- Foreign national restrictions
- Export control clauses
- Security requirements
- Government approval provisions
- Proprietary information clauses

18.3 Proposal Stage Review

Investigators should consult the ECO before proposal submission when projects involve:

- Defense sponsors
- International collaborators
- Controlled technologies
- Foreign governments
- Classified work

18.4 Award Acceptance

Prior to award acceptance, the ECO may evaluate:

- Export licensing needs
- Technology Control Plans
- Equipment restrictions
- Data restrictions
- International participation

Chapter 19 - Procurement and Purchasing

19.1 Purpose

Purchasing activities may create export control obligations when acquiring controlled equipment, software, biological materials, or technology.

19.2 Purchases Requiring Review

Examples include:

- Lasers
- Thermal cameras
- UAV systems
- Satellite hardware
- Controlled chemicals
- Encryption software
- Advanced computing systems

19.3 Vendor Screening

International vendors may be subject to Restricted Party Screening.

19.4 Receiving Controlled Equipment

Departments should notify the ECO when receiving export-controlled equipment.

Chapter 20 - Information Security and Controlled Research Data

20.1 Overview

Information security is an essential component of export control compliance.

20.2 Controlled Information

Examples include:

- Export-controlled technical data
- Controlled Unclassified Information (CUI)
- Sponsor-restricted information
- Proprietary information
- Sensitive research data

20.3 Minimum Security Controls

Projects may require:

- Encryption
- Multi-factor authentication
- Secure file storage
- Role-based access
- Audit logging
- Secure backups

20.4 Cloud Computing

Only institutionally approved cloud services should be used for controlled information, and only when consistent with applicable regulatory and contractual requirements.

20.5 Incident Reporting

Loss or unauthorized disclosure of controlled information shall be reported immediately to:

- Information Security Office
 - Export Control Officer
 - Office of Research Integrity
-

Chapter 21 - Recordkeeping Requirements

21.1 Purpose

UNLV shall maintain export control records sufficient to demonstrate institutional compliance.

21.2 Records

Examples include:

- License applications
- License determinations
- Screening records
- Shipping documentation
- TCPs
- Training records
- Contracts
- Equipment inventories

- Travel reviews

21.3 Retention

Records shall be retained in accordance with applicable federal regulations, sponsor requirements, NSHE records policies, and University records retention schedules. Where multiple requirements apply, the longest applicable retention period should be observed unless otherwise directed by law or policy.

Chapter 22 - Compliance Monitoring and Audits

22.1 Internal Reviews

The Export Control Office shall periodically review institutional compliance activities.

22.2 Audits

Audits may include:

- Research laboratories
- International collaborations
- Shipping activities
- Technology Control Plans
- Sponsored research

22.3 Corrective Actions

Corrective actions may include:

- Additional training
 - Policy revisions
 - Increased monitoring
 - Self-disclosures when appropriate
-

Chapter 23 - Violations and Enforcement

23.1 Reporting Violations

Potential violations shall be reported immediately to the Export Control Officer.

23.2 Internal Investigation

The University will investigate suspected violations and determine appropriate corrective actions.

23.3 Voluntary Self-Disclosure

When appropriate, UNLV may submit voluntary self-disclosures to the responsible federal agency after consultation with University leadership and legal counsel.

23.4 Institutional Discipline

Violations may result in:

- Loss of research privileges
- Corrective action
- Employment discipline
- Student disciplinary action
- Contract termination

23.5 Federal Penalties

Violations of export control laws may result in significant civil and criminal penalties, including monetary fines, denial of export privileges, and imprisonment. Applicable penalties are established by federal statute and regulation and may change over time. The Export Control Office should maintain current reference materials reflecting applicable enforcement authorities.

Chapter 24 – Definitions

Commerce Control List (CCL) - a list maintained by BIS that identifies items subject to the EAR and assigns them Export Control Classification Numbers (ECCNs) based on their technical characteristics and reasons for control.

Commodity - Any article, material, or supply except technology and software

Controlled Unclassified Information (CUI) - Government-created or government-owned information that requires safeguarding or dissemination controls pursuant to federal laws, regulations, or government-wide policies but is not classified. CUI is not automatically subject to export controls but may contain export-controlled information.

Deemed Export - The release or disclosure of controlled technology or source code to a foreign person within the United States. Under the EAR, such a release is considered an export to the individual's country of citizenship or permanent residence.

Defense Article - Any item, technical data, software, or component specifically designed, developed, configured, adapted, or modified for a military, intelligence, or space application and listed on the U.S. Munitions List (USML). Defense articles are regulated under the International Traffic in Arms Regulations (ITAR).

Dual Use Items - are controlled under the EAR and used in military and civilian applications

EAR (Export Administration Regulations) - found at 15 C.F.R. Parts 730–774, which govern the export, reexport, and transfer of commercial and dual-use items, software, and technology under the jurisdiction of the U.S. Department of Commerce.

Export - the transfer of export-controlled data, items, equipment, materials, and software or providing a defense service to a non-U.S. Person or entity. An export can occur in a number of ways, such as; a physical shipment, hand-carrying an item out of the U.S., email transmission of data, presentations, discussions, or visually accessing export-controlled data.

Foreign National - an individual who is not a United States citizen, permanent resident alien of the United States (i.e., “green card holders”), lawfully admitted temporary resident alien or refugee, or other protected individual as defined by 8 U.S.C. 1324b(a)(3).

Fundamental Research (under the EAR) - research in science, engineering, or mathematics, the results are ordinarily published and shared broadly within the research community, **and** the researchers have not accepted restrictions for proprietary or national security reasons.

Fundamental Research (under the ITAR): research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community, as distinguished from results restricted for proprietary reasons or specific U.S. government access and dissemination controls. Research will not be considered fundamental research if: (i) the university or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or (ii) the research is funded by the U.S. government and specific access and dissemination controls protecting information resulting from the research are applicable.

Fundamental Research Exclusion (FRE) - An exclusion from export control licensing requirements that applies to information resulting from fundamental research, provided there are no publication restrictions or restrictions on participation by foreign nationals. The exclusion does not apply to tangible exports, controlled equipment, encrypted software, or certain defense services.

ITAR (International Traffic in Arms Regulations) - Regulations administered by the U.S. Department of State (22 C.F.R. Parts 120–130) governing defense articles, defense services, and related technical data listed on the U.S. Munitions List.

Office of Foreign Assets Control (OFAC) - a division of the U.S. Department of Treasury, which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the U.S.

Restricted Party Lists - a series of lists published by the U.S. Departments of Commerce, Treasury, and State as well as the General Services Administration, which identify the names of companies and individuals to whom there exists restrictions upon the ability to export controlled items. These lists include the Denied Persons List, the Unverified List, the Entity List, the Specially Designated Nationals List, the Debarred List, and the Excluded Parties List.

Software - A collection of one or more “programs” or “microprograms” fixed in any tangible medium of expression.

Technology - Under the EAR, specific information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishment of an item. Technology may take the form of technical data or technical assistance.

Technology Control Plan (TCP) - A written institutional plan describing the physical, electronic, and administrative safeguards used to prevent unauthorized access to export-controlled items, technology, software, or technical data by foreign persons or other unauthorized individuals.

U.S. Munitions List (USML) - A list maintained by the U.S. Department of State identifying defense articles, defense services, and related technical data subject to the ITAR.

Chapter 25 – Appendices

Appendix A

Applicable Federal Regulations

- Export Administration Regulations (15 CFR Parts 730–774)
- International Traffic in Arms Regulations (22 CFR Parts 120–130)
- OFAC Regulations (31 CFR Chapter V)
- NSHE Chapter 14 Export Control and Economic Sanctions Policy

Appendix B

Revision History

Version Number	Effective Date	Author	Summary of Revisions
1	08/01/2026	Chelsea Holmes	Creation of Export Control Manual