OLD DOMINION UNIVERSITY
University Policy

Policy # 5340
EXPORT CONTROL, SANCTIONS, AND NATIONAL SECURITY PROGRAM POLICY

Responsible Oversight Executive: **Vice President for Research and Economic Development**
Date of Current Revision: **June 1, 2026**

A. PURPOSE

This policy outlines Old Dominion University's (ODU) mandatory compliance with U.S. export control laws and trade sanctions, which protect national security and international interests. These regulations apply to all university academic, research, and business activities, including the transfer of controlled items, technology, software, and information; collaborations with foreign entities; and engagements with restricted parties or sanctioned countries. The U.S. Government enforces export control regulations and trade sanctions through civil and criminal penalties for both individuals and the University, including fines, imprisonment, debarment, or loss of export privileges and federal funding. The policy emphasizes a culture of compliance and supports coordinated efforts through the Office of Research Security and Export Control (ORSEC) and the Old Dominion University Research Foundation (ODURF).

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 7.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

- Export Administration Regulations (EAR) — 15 CFR 730-774
- International Traffic in Arms Regulation (ITAR) — 22 CFR 120-130
- Office of Foreign Assets Control (OFAC) — 31 CFR 500, Subtitle B, et seq.
- Department of Energy Regulations — 10 CFR 110 and 810, et seq.
- NISPOM — 32 CFR 117
- Controlled Unclassified Information — 32 CFR 2002, EO 13556

C. DEFINITIONS

Affiliate: Individuals or organizations acting on behalf of the University but organized as a separate legal entity.

Controlled Unclassified Information (CUI): Information that the Government, or an entity on behalf of the Government, creates or possesses that requires safeguarding or dissemination controls when handling (32 CFR 2002, Executive Order 13556).

Commerce Control List: A list of "dual-use" items, materials, software, and technology, subject to export regulation, maintained by the Department of Commerce.

Deemed Export: Release of Export Administration Regulation regulated source code or controlled technology to a foreign national in the United States or abroad is "deemed" to be as if it were released to that foreign national's country of origin.

Defense Article: Any item or technical data that is specifically designed, developed, configured, adapted, or modified for a military, missile, satellite, or other controlled use listed on the USML. Defense articles also include things such as models, mock-ups, or other items, i.e. technical data related to items. Note that sometimes defense articles include items not listed on the USML.

Defense Service: Furnishing technical data or assistance (including training) to Foreign Persons (i.e., foreign nationals), whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles, or military training of foreign units and forces.

Empowered Official: Is a registered U.S. person who is legally empowered in writing by the University to sign ITAR export license applications or other requests for approval on behalf of Old Dominion University; who understands the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability, and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations.

The Empowered Official is a senior level administrator within the Division of Research and Economic Development.

Export: International transfer of any commodity, software, material or technology (information) including (but not limited to) specifically "export controlled" items (as defined by Government agencies) by any means including (but not limited to) courier/mailed shipment, hand carried transfer, digital transfer, spoken communication and, (depending on the export control level) visual access to certain controlled items and information.

Export Administration Regulations (EAR): A set of U.S. Government regulations administered by the Bureau of Industry and Security at the Department of Commerce that control the export, reexport, and transfer of commercial and dual-use items on the Commerce Control List (15 CFR 730-774).

Export License/Authorization: Official written approval by a governing agency to conduct a particular export or deemed export transaction.

Export Recordkeeping: Federally required 5-year export-related record retention.

Facility Security Officer (FSO): A designated senior level administrator within the Division of Research and Economic Development responsible for supervising and directing security measures necessary for implementing the applicable requirements of the 32 CFR part 117 (NISPOM) and the related USG security requirements to ensure the protection of classified information.

Foreign Persons: Any individual who is not a U.S. citizen, a lawful permanent resident of the U.S., or a "protected individual" (i.e. asylees or refugee status).

International Traffic in Arms Regulations (ITAR): The Department of State's Directorate of Defense Trade Controls (DDTC) export control regulations governing access to and use of defense items and technologies domestically and internationally, as well as delivery of codified defense services to international defense agencies (22 CFR 120-130).

National Industrial Security Program Operating Manual (NISPOM): Security procedures and practices that are required by all government contractors when they are granted access to or develop classified information for the U.S. government (32 CFR 117).

Office of Foreign Assets Control (OFAC): Branch of U.S. Treasury Department which exercises oversight over U.S. Government's trade sanctions and embargo programs. (31 CFR 500, Subtitle B, et seq.)

Restricted Party Screening (RPS): On-line accessible, screening procedure using Old Dominion University's Visual Compliance licensed software tool to determine whether individuals and entities with whom the University engages are identified/listed on any of the U.S. Government's restricted party lists.

Technology Control Plan (TCP): Documented, comprehensive security measures applicable to federal and industry-sponsored research and service agreements and contracts where Old Dominion University is an award recipient or subcontractor, and agreement/contract mandates, export control restrictions, and/or dissemination restrictions; and/or special engagement; and/or data security restrictions (including but not limited to U.S. Government governed classified contracts).

Trade Sanctions: Specific prohibition under the OFAC regulations governing engagement with OFAC-sanctioned ("blocked") parties as well as broad country defined restrictions (e.g. Cuba, Iran, Syria, North Korea, Russia).

Voluntary Self-Disclosure: Procedure to timely report export control/trade sanction violations to the appropriate federal agency.

D. SCOPE

The University is committed to complying with applicable export control laws, trade sanctions, and national security regulations. To comply with the aforementioned regulations, this policy applies to all Old Dominion University personnel, including students, faculty, staff, administrators, visitors, and courtesy faculty appointments conducting any research, academic, or business activity on behalf of Old Dominion University or otherwise associated with Old Dominion University. This policy applies to the identification and compliance with export control and national security regulations and related procedures. Technical requirements are not within the scope of this policy.

E. POLICY STATEMENT

All University personnel, students, visitors and courtesy faculty appointments conducting any research, academic, operational/administrative, business activity, or University affiliates on behalf of Old Dominion University or activities that may result in an export or sanctioned transaction, protection and management of United States Government classified information under the National Industrial Security Program (32 CFR 117), and administrative compliance with safeguarding Controlled Unclassified Information (32 CFR 2002) shall also, respectively, comply with Old Dominion University's Export Compliance and Trade Sanctions procedures. This policy is subject to all applicable federal and state regulations. If any part of this policy conflicts with a regulation, the regulation shall take precedence.

Research Controlled Unclassified Information

The Controlled Unclassified Information (CUI) Program (Executive Order 13556 and 32 CFR 2002) requires safeguarding to prevent the unauthorized release of covered information. The covered information includes all research information determined to be CUI by the contract, grant, or agreement.

National Security Related Research

The National Industrial Security Program includes all national security related research related transactions involving the facility clearance, personnel clearances, and access to classified materials and equipment subject to the NISPOM (32 CFR 117), other applicable national security issuances, and Executive Orders for the protection of classified information.

Export Control and Sanctions

The Export Control and Sanctions program includes all export and sanctions related activity within Old Dominion University.

Common Research and Academic Activities with Associated Export Control Requirements
Activities Covered include but are not limited to:

Research Proposals and Pre-award Activity: When developing a proposal for research, including sponsored and unfunded research, confer with the Office of Research Security & Export Control (ORSEC) about potential export compliance requirements as well as international activities requiring disclosure in the proposal.

Scholarship and Collaborations: When engaging in research and scholarship with international entities, the Office of Research Security and Export Control should screen for restricted parties and other export regulated activity.

Technology Sharing: Certain items used in fundamental research including instruments, software, materials, and technical data may be export controlled, even if the research itself is fundamental research (i.e. not otherwise publication or citizenship restricted). Sharing export-controlled technology pertaining to such items with Foreign Persons may, depending on the person's citizenship, constitute a "deemed export" requiring specific U.S. Government authorization prior to sharing the technology. If such requirements are not already specified in a Technology Control Plan (TCP) covering your item or activity or you are unsure about whether such requirements apply, seek guidance from the Export Control Office on Controlled Information.

International MOUs and MOAs: These types of institutional agreements with international partners must include a Restricted Party Screening.

Visa Petitions: When planning to host new visa candidates or individuals with existing visas, hosts are required to complete the Deemed Export Questionnaire that helps determine whether there are deemed export issues associated with the Foreign Person's research work or potential access.

International Travel: All proposed international travel to a sanctioned or high-risk country (as defined in the Department of State Country of Concern list) must be reviewed and approved by the Export Control Office. All international research travel is reviewed. Travel to high-risk destinations will go through a risk assessment and export control review before travel is approved. After review, the Office of Research Security and Export Control will proactively coordinate any special export control measures pertaining to the planned travel, to include assisting with licensing determinations, OFAC restrictions, and risk mitigations.

Engagement with U.S. Treasury Department Trade-sanctioned Countries: When planning travel to or engaging with any person or entity located in one of the broadly sanctioned countries, proactively contact the Export Control Office at least 60 days in advance of such travel or engagement to determine whether Treasury Department authorization is required.

Related Areas Potentially Involving Export Compliance:

Conflict of Interest/Conflict of Commitment Reporting: Any activity that is disclosed on a Conflicts of Interest and/or Conflicts of Commitment report, which involves an international individual or entity, must be reviewed by the Export Control Office prior to approval by the Conflicts Office and/or other designated approver.

Technology Licensing to International Parties: The Office of Innovation and Commercialization partners closely with the Export Control Office to perform technology and licensee reviews as needed.

International Donors and Gifts: The Export Control Office partners with the Research Foundation to identify and review gift transactions with international donors. The Research Foundation does not collect or receive gifts; the foundation serves as the reporting entity on behalf of ODU.

F. PROCEDURES

All changes and additions to federal and state regulations covered by this policy will take precedence. The Office of Research Security and Export Control is responsible for staying up to date with regulatory updates and making changes to the compliance program in accordance with the applicable regulations. The Office of Research Security and Export Control will annually review processes and the Export Control, Sanctions, and National Security Program Manuals.

Export Control and Sanctions Compliance Program
This policy, the Old Dominion University Export Compliance Manual, and subordinate procedures outline and describe the Old Dominion University Export Compliance Program. Activities performed by ORSEC include but are not limited to:

- Release or transfer of technology, source code, or technical data to a Foreign Person or Entity in the United States
- Transactions subject to the General Provisions of the EAR
- Performing a defense service on behalf of, or for the benefit of, a Foreign Person
- International collaborations or academic exchanges with sanctioned countries, entities, and individuals

Industrial Security Compliance Program
This Policy and the Old Dominion University Classified Program Standards, Processes and Procedures outline and describe the Old Dominion University National Industrial Security Program. Activities performed by ORSEC include but are not limited to:

- Designating an FSO and ensure the institution remains eligible and approved to access and store classified information
- Ensuring individuals accessing classified information have Personnel Security Clearances (PCLs) and are properly vetted
- Establishing a Standard Practice Procedure document for the University in accordance with the NISPOM (32 CFR 117)
- Provide initial and annual security awareness training to all cleared personnel
- Conduct self-inspections, at minimum, annually
- Disclose any foreign ownership, control, or influence over the University that could affect the University's ability to protect classified information

The Old Dominion University Research Foundation maintains a separate facility clearance to the University. ODU Facility Security Office and the Research Foundation Facility Security Officer coordinate and align processes.

Responsibilities

Office of Research Security and Export Control

The Division of Research and Economic Development Office of Research Security and Export Control is responsible for overseeing day-to-day export compliance and implementing the export compliance and trade sanctions program. ORSEC, through the University Empowered Official, is responsible for approving and directing international exports of export-controlled items and any transaction that may be subject to federal export and sanctions regulations. ORSEC is responsible for administrative compliance with safeguarding Controlled Unclassified Information (CUI) and Research CUI determinations. ORSEC is responsible for the management and administration of the ODU Facility Clearance and accreditation of facilities necessary to conduct national security related academic and research activity. ORSEC serves as the Facility Security Officer (FSO) and Insider Threat Program Senior Official (ITPSO) as required by the NISPOM (32 CFR 117). ODU Facility Security Office coordinates with the ODU Research Foundation FSO to align processes with the ODU Facility Security Program.

ORSEC shall timely inform the University's executive leadership of any suspected or potential violations pertaining to export, CUI, or NISP compliance.

Faculty, Staff, and Students

Old Dominion University's faculty, staff, and students are responsible for ensuring that their educational, research, and other business activities involving international collaborations and foreign exchanges are conducted in compliance with U.S. export, sanctions, or security regulations and any procedures identified herein or in a Technology Control Plan. If faculty, staff, or students are involved in classified research, controlled unclassified research, international collaborations, or foreign exchanges with risk of export control, sanction, or security regulation violation, they will comply with the provisions of any license, government approval, policy, or OESRC-directed certification, Technology Control Plan, or other procedure.

G. COMPLIANCE

Failure to comply with U.S. federal export control laws can result in significant civil and criminal penalties for both the individual and the University, including substantial fines, imprisonment, loss of export privileges, federal funding, or debarment.

H. RECORDS RETENTION

Records related to export-controlled activities must be retained in accordance with federal requirements. Documentation for projects subject to the ITAR and the EAR must be maintained for a minimum of five years from the date of the export or the completion of the activity, whichever is later. Records pertaining to compliance with OFAC regulations must be retained for at least ten years.

I. RESPONSIBLE OFFICER

Assistant Vice President for Research Security and Export Control

J. RELATED INFORMATION

15 CFR 130
15 CFR 120-130
31 CFR 500-599
10 CFR 110
10 CFR 810
NISPOM
32 CFR 2002
Conflicts of Interest Policy 5201

POLICY HISTORY

****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ David Flanagan — June 1, 2026
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Heidi G. Smith — June 1, 2026
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Kenneth Fridley — June 1, 2026
Responsible Oversight Executive — Date

University Counsel Approval to Proceed:

/s/ Allen T. Wilson — June 1, 2026
University Counsel — Date

Presidential Approval:

/s/ Brian O. Hemphill — June 1, 2026
President — Date

Policy Revision Dates: **June 12, 2013; October 1, 2020; June 1, 2026**

Scheduled Review Date: **June 1, 2031**