

UVA Research Open Forums



Join us for the UVA Research Open Forum Series!

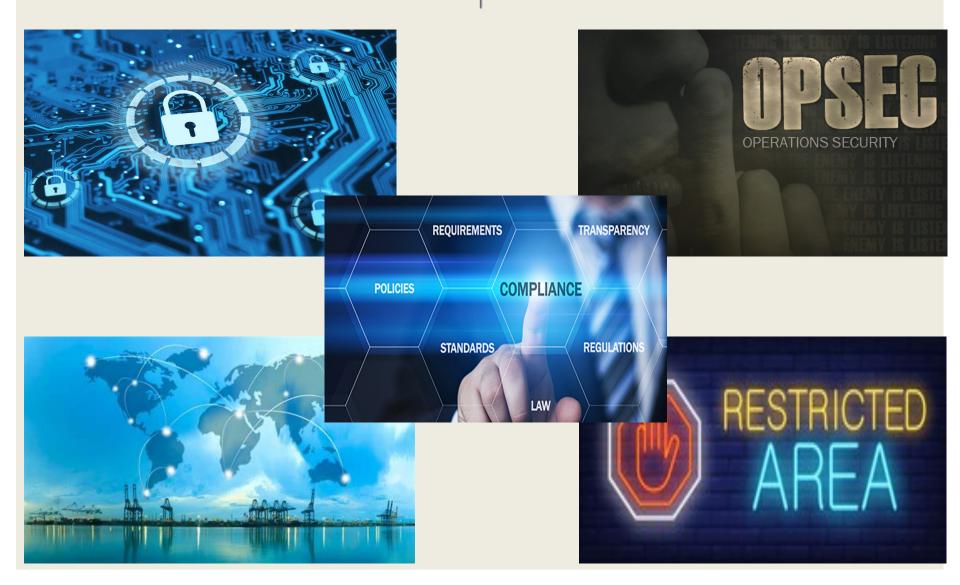
To help keep the UVA Research community updated and gain feedback on future improvements, the OVPR will host multiple **Open Forums**.

- November 20: OSP Pre-Award
- NEW: December 4: OSP Post-Award





Vice President for Research Office of Research Security



OFFICE OF RESEARCH SECURITY

Office of Vice President for Research
 Office of Research Security
 Chief Research Security Officer - Rob Jones

Program Areas:

- Export Controls Program LaVerne Grant
- Research Data Security Andrew Bedotto
- Foreign Influence/Classified Programs Jonathan Velasquez
- Operational Security (OPSEC) Rob Jones/Jonathan Velasquez

Office of Research Security Website - https://security.research.virginia.edu/

- General Information for Each Program Area
- Procedures & Forms
- Information on Training Options
- Report Problems or Concerns

EXPORT CONTROLS

Laws, regulations and multilateral agreements governing:

- The export, reexport, and transfer
- By U.S. and foreign persons
- Of commodities, technology, software, and services (WHAT)
- To destinations, end uses, and end users (WHERE)/(WHO)
- To accomplish various national security and foreign policy objectives

Policy FIN-043: Managing Export and Sanction Compliance in Support of University Activities -

https://uvapolicy.virginia.edu/policy/FIN-043

HOW MIGHT EXPORT CONTROLS APPLY TO UNIVERSITY ACTIVITIES?

- Terms and Conditions of Awards or Other Agreements
- Traveling Internationally with University Equipment (laptop, cell phone, research material)
- Shipping Research Materials to International Colleagues (US or Abroad)
- Collaborating with research partners who are non-US persons
- Use of certain controlled items to conduct the research
 - Note: New controlled items are added continuously
- A controlled item is the subject of the research
- Use of controlled background information
- Activities conducted outside the US
- Exports to or involving a restricted or denied party (i.e. an entity identified on one of several US Government lists)
- Activities involving sanctioned countries

2024 CRITICAL AND EMERGING TECHNOLOGIES

The following critical and emerging technology areas are of particular importance to the national security of the United States:

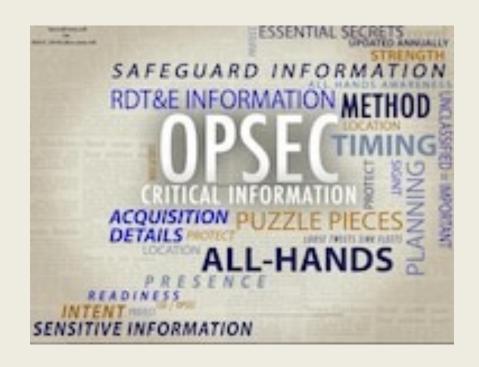
- Advanced Computing
- Advanced Engineering Materials
- Advanced Gas Turbine Engine Technologies
- Advanced and Networked Sensing and Signature Management
- Advanced Manufacturing
- Artificial Intelligence
- Biotechnologies
- Clean Energy Generation and Storage
- Data Privacy, Data Security, and Cybersecurity Technologies
- Directed Energy
- Highly Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics
- Human-Machine Interfaces
- Hypersonics
- Integrated Communication and Networking Technologies
- Positioning, Navigation, and Timing (PNT) Technologies
- Quantum Information and Enabling Technologies
- Semiconductors and Microelectronics
- Space Technologies and Systems

EXPORT CONTROLS SUMMARY

- Export controls apply to a wide range of items, information, activities and services – and many University activities!!!
- Do not assume your research does not require further review and approval or other authorizations.
- Potential Penalties for non-compliance are severe for the institution and for individuals Ignorance of the specifics of the law has not been a successful defense in export control cases.
 - Criminal and Civil Penalties for INDIVIDUALS including major fines and jail time
- Contact the UVA Office of Research Security for assistance or if you have questions or concerns- export-controls@virgnia-edu

OPERATIONAL SECURITY

A process that managers can use to protect critical/sensitive information from falling into the wrong hands.

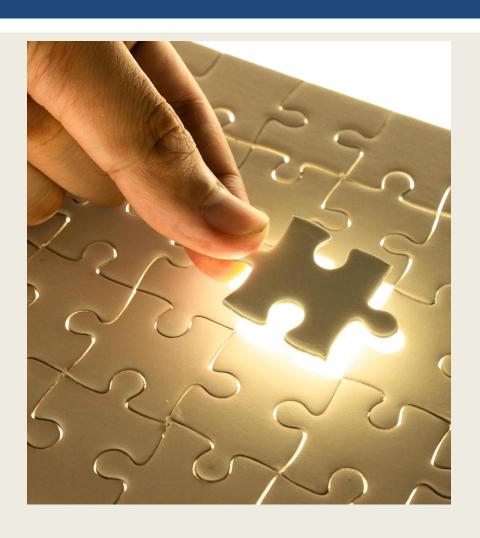


OPSEC FIVE STEP PROCESS

- 1. Identify critical & sensitive data
- 2. Analyze the threat
- 3. Determine the vulnerabilities
- 4. Assess the risk
- 5. Mitigate or eliminate the threats



WHAT IS CRITICAL INFORMATION



- It can be unclassified or control unclassified information (CUI) about activities, intentions, capabilities, or limitations
- It can include indicators... specific facts that an adversary seeks to collect, analyze and exploit to gain some type of advantage.
- Can be revealed by Publicly Available Information (PAI)

THREATS AND VULNERABILITIES

Threats

- Can be anyone with the intent and capability to take actions detrimental to the success of activities and operations.
 - Foreign Governments
 - Sworn Enemies
 - Terrorists
 - olnsiders

Vulnerabilities

- OPSEC vulnerability exists when the adversary is capable of collecting critical information to exploit our vulnerabilities.
 - Observation
 - Internet (Social Media)
 - **Ounsecure Comms**
 - Pattern of Life

ASSESSING & MITIGATING RISKS

Assessment

- Determine Level of Risk
 - Adversaries' abilities
 - OPotential Impact
- A decision-making step to determine if countermeasures need to be assigned.

Mitigation/Elimination

- Happens after a risk assessment is conducted
- If risk is determined to be unacceptable establish countermeasures to
 - o Mitigate risk, or
 - Establish acceptable level of risk

FOREIGN INFLUENCE

- Foreign Influence Definition
 - •Efforts by foreign governments, organizations, or individuals to sway or impact US policies, decisions, or activities to serve their own interests.

FOREIGN INFLUENCE EXAMPLES

- Foreign Government-Sponsored Talent Programs (FGTPs)
- Theft of Intellectual Property (IP)
- Diversion of intellectual capital developed in US-funded research institutions (NCURA 2023).

FOREIGN INFLUENCE AREAS OF CONCERN

- Non-financial Conflict of Interest
 - **OUVA** Policies
 - FIN-054: Employee Obligations to Report Conflicts of Interest
 - FIN-055: Faculty and Staff International Travel

- Conflict of Commitment
 - Security of intellectual property
 - •Integrity of peer review (NCURA 2023)
 - Finacial Conflicts of Interest
 - RES-005: Financial Conflicts of Interest for Research Investigators
 - Establishment of foreign labs, Honorariums, etc...

CLASSIFIED PROGRAMS

- You will know when you are part of one!
- Classified information is material that if made public could endanger US National Security.
 - Confidential
 - Secret
 - Top Secret
- Safeguards and access restrictions
- Typically, some type of "Read On" occurs.
- A Security Clearance Investigation and background are be part of the process.
- Restrictions and guidance is defined by the Government customer.
- Operate on a "Need to Know" basis.
- Everything you hear in this presentation is taken up a notch!

WHAT RDS DOES

- Assists with research data acquisition and sharing
- Review and implementation of data use agreements and sponsored projects involving sensitive data
- Implementation of data protection standards such as Controlled Unclassified Information (CUI), Export Controlled information, and Human Subjects data
- Guidance on traveling internationally with University owned, controlled, or managed data.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

- Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable FEDERAL law, regulations, and government-wide policies, but is not classified
- CUI includes various types of information not all of which is export controlled.
 - Student records, Health information, Immigration records, Federal Tax Information
- CUI must be transmitted, stored, and destroyed in accordance with NIST 800-171.
- CUI must be labeled appropriately.
- If you receive CUI via email, DON'T OPEN THE ATTACHMENT, CALL ME!
- If CUI is part of one of your proposals or awards, I'II CALL YOU!

RDS HIGHLIGHTS

- RES-002: Ownership, Retention, Safeguarding, Management, and Transfer of Research Records
- Unpublished fundamental research data is sensitive data according to the University Data Standards
- Research records must be maintained under University control
- Electronic research records must be maintained on Universityowned/managed devices
- Know the Data Protection Standard of the research data in your possession

RDS UPDATES

- January 25, 2025
 - NIH Database of Genotypes and Phenotypes (dbGaP) transition to a new, more secure standard (NIST 800-171)
 - Applies to new or renewed Data Use Certifications or similar agreements
 - Data is Controlled Unclassified Information (CUI)
- October 1, 2025
 - Cybersecurity Maturity Model Certification (CMMC) requirements included in in all DoD solicitations and contracts or task orders or delivery orders.
 - Phased Implementation over 3 years
 - Awaiting FAR final rule 48 CFR 204 to be published to begin timeline