NSF Research Security Training
Module 1: What is Research Security? QRG

Objective: By the end of this module, you will be able to define research security, explain why it's important, identify key federal research security guidance, and recognize warning signs of malign foreign influence.

What is research security and why is it important? Research security is the collective system of controls that safeguards the research enterprise against threats to national and economic security, integrity breaches, and foreign interference.

By practicing research security, we ensure that our research findings and innovations are safe from theft or misuse. If researchers protect their work, the U.S. will continue to inspire innovation, encourage investment in research and development, and maintain a culture of trust and collaboration.

Research security benefits us by:

- Safeguarding sensitive information and technological advances
- Preventing bad actors from harming our own research
- Protecting our national security
- Keeping IP and innovations from theft or misuse
- Encouraging innovation and investment in research and development
- Maintaining a good reputation and a culture of trust and collaboration

Key federal research security guidance:

- **JASON report** – requires full disclosure of all potential conflicts of interest and recommends investigating all non-compliance issues as research misconduct.
- **National Security Presidential Memorandum (NSPM-33)** – requests standardized disclosure requirements, requires using Digital Persistent Identifiers (DPIs), mandates a research security program, and provides guidance for sharing breaches among federal funding agencies.
- **Chips and Science Act** – boosts investments in research and development to bring preeminence in semiconductor manufacturing back to the U.S. It mandates the NSF establish a research security and integrity information sharing and analysis clearinghouse for all stakeholders. It also is to develop best practices and a risk assessment framework and provide research security training as a part of Responsible Conduct of Research (RCR) training. The act pushes for prohibiting membership in any malign foreign talent program.
- **Research Security Programs Standard Requirements** – NSTC guidance specifies research organizations must certify annually that they have a research security program meeting the requirements, this program must also have training on foreign travel security, research security, cybersecurity, and export control.

Core values

All research conducted must be consistent with the core values. The core values are openness and transparency, accountability and honesty, impartiality and objectivity, respect, freedom of inquiry, reciprocity, and merit-based competition. More information on the core values can be found in module 4.

Warning signs of malign foreign influence:

- Non-compliance with the core values
- Employment by a foreign entity
- Foreign funding of similar research
- Provision of free or subsidized labor
- Talent programs
- Equity interests in closely held research companies
- Non-disclosure agreements
- Asking to provide information they otherwise would not have access to, especially in exchange for benefits or improper, often under the table, payment
- Threats of harm

Roles of various groups in research security:

- **The PI and research team** – decides whether to collaborate and with whom by weighing the risks and benefits of working with another scientist whether in the U.S. or outside of it. PIs are also required to disclose potential conflicts of interests and need to persistently divulge all relationships, investments, employment, and consultancies that may impact research security.
- **Research administrators** – help the researcher navigate the administrative aspects of sponsored projects. They monitor and maintain consistent compliance with research security requirements, including disclosure requirements. Serve as a point of contact for the PI to connect them to the right person when they have questions.
- **Research leadership and senior officials** – create research security awareness and a culture of compliance by establishing clear and comprehensive policies and procedures, including disclosure policies, reviewing and reconciling potential issues, and taking a lead role in working with federal agencies.
- **Federal government** – creates administrative policies and laws and ensures they are properly implemented and complied with. This includes harmonizing policies and regulations across agencies.
- **Federal funding agencies** – evaluate disclosures, set guidelines, and monitor compliance with established security protocols.

Research security concerns:

- **International travel** – avoid inadvertently exposing sensitive information to those who have malicious intent. Before traveling, thoroughly assess and mitigate the

risks of data theft with the help of research administrators. While abroad, avoid discussing sensitive research topics with any who aren't your most trusted partners.
- **Intellectual property –** contact your institution's technology transfer professionals to evaluate anticipated products from the research and determine if patents or confidentiality agreements are necessary. Loosely secured data can be stolen, and it is very difficult to prove IP infringement.

Security breaches

A security breach includes things like data theft, sharing confidential proposals or protected results, or granting access to shared drives and cloud services without their organization's awareness or approval. In the event of a security breach, research administrators notify the appropriate institutional officials and work closely with the PI, institutional officials, and the sponsor to diligently investigate the issue. The research leadership team will also engage the sponsors and federal government to disclose and resolve inquiries and cases. Most important in the case of a security breach is openness, transparency, and timeliness to resolve the problem as quickly and effectively as possible.

Consequences of security breaches:

- Criminal charges
- Civil liabilities
- Debarment
- Large fines
- Reputational harm
- Increased concern and doubt about international collaborations in general which can delay scientific and technological advancement