NIST Safeguarding International Science Research Security Framework

NIST IR 8484

Presented by Gregory Strouse,
NIST Research Security Team Lead

Team Members:

Claire Saundry, International and Academic Affairs
Timothy Wood, Export Control
Blair Heiserman, Chief Information Security Officer
Philip Bennett, Research and Technology Protection

Team e-mail: researchsecurity@nist.gov

Agenda

- Defining Safeguarding International Science
- Framework objectives
- Overview of the NIST Safeguarding International Science Research Security Framework
- Fundamental constructs of the Framework
- Observations and lessons learned
- Challenges and points for consideration by the U.S. science and research community
- Framework test case
- Q&A

Safeguarding International Science Research Security Framework

Safeguarding International Science

Achieve a balance between open scientific collaboration and research security that values collaboration while protecting U.S. intellectual property

Objectives

Establish a national research security review platform for to assist the U.S. science and research community across the broad spectrum of international science and technology activities as well as Federal funding initiatives.

Enable organizations to implement a mission-focused, integrated, risk-balanced program through the application of research security principles and best practices that fosters the safeguarding of international science while mitigating risks to the integrity of the open collaborative environment.

Enables an organization to meet NSPM-33 Research Security program certification requirements.

NIST IR 8484 – Safeguarding International Science Research Security Framework

Framework Development

Outcome of 3+ years of collaborative engagement across the research security enterprise

- NIST leadership and staff researchers
- Multiple NT-50 Partner Agencies
- ODNI (NCSC) Safeguarding Science Roundtable
- International Metrology Institutes

Implementation

- Strategic Communication and Training
- Composite Mutli-Disciplined Open-Source Analysis
- Risk Balanced Operations Security (NSPM-28) methodology
- User friendly tools, checklists, and templates

Holistic / Scalable / Deployable / Non-intrusive

NIST Internal Report
NIST IR 8484

Safeguarding International Science

Research Security Framework

Gregory F. Strouse
Office of the Associate Director for Laboratory Programs
Laboratory Programs

Philip A. Bennett
Research and Technology Protection
Commerce Office of Security

Timothy R. Wood
Research Protections Office
Laboratory Programs

Mary Bedner
CHIPS Research and Development Program
CHIPS Program Office

Claire M. Saundry
International and Academics Affairs Office
Director's Office

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8484

August 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

https://doi.org/10.6028/NIST.IR.8484

Community Milestone

Safeguarding Science Toolkit
September 2022

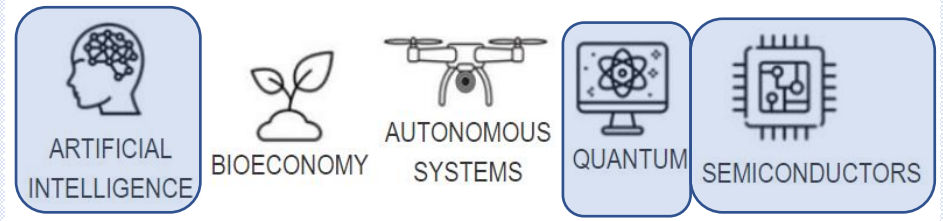
- Promote a U.S. research ecosystem that emphasizes collaboration, openness, equity, integrity, and security, all of which facilitate innovation
- Provide curated resources for our stakeholders to support best practices in protecting research and innovation
- Assist academia and industry in developing their own methods to protect research from theft, misuse, abuse, or exploitation
- Foster information exchanges to better identify emerging technology security challenges

Office *of the* Director *of* National Intelligence

The National Counterintelligence and Security Center

Safeguarding Science

An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies



National Science Foundation

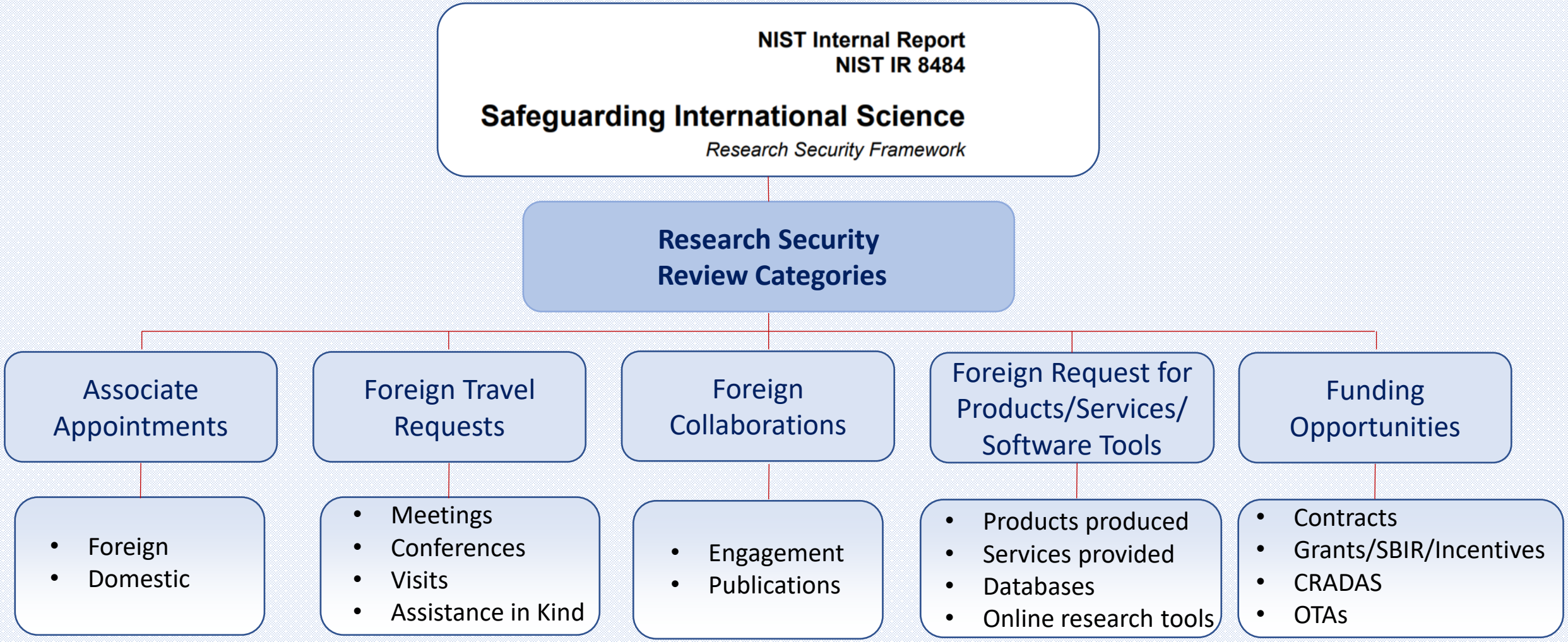
NIST National Institute of Standards and Technology U.S. Department of Commerce

Federal Aviation Administration

- Research Security
- Academic Resources
- Cybersecurity
- Operations Security
- Counterintelligence
- Insider Risk
- Supply Chain Risk Management
- Threat Information
- Information Security
- Personnel Security
- Physical Security

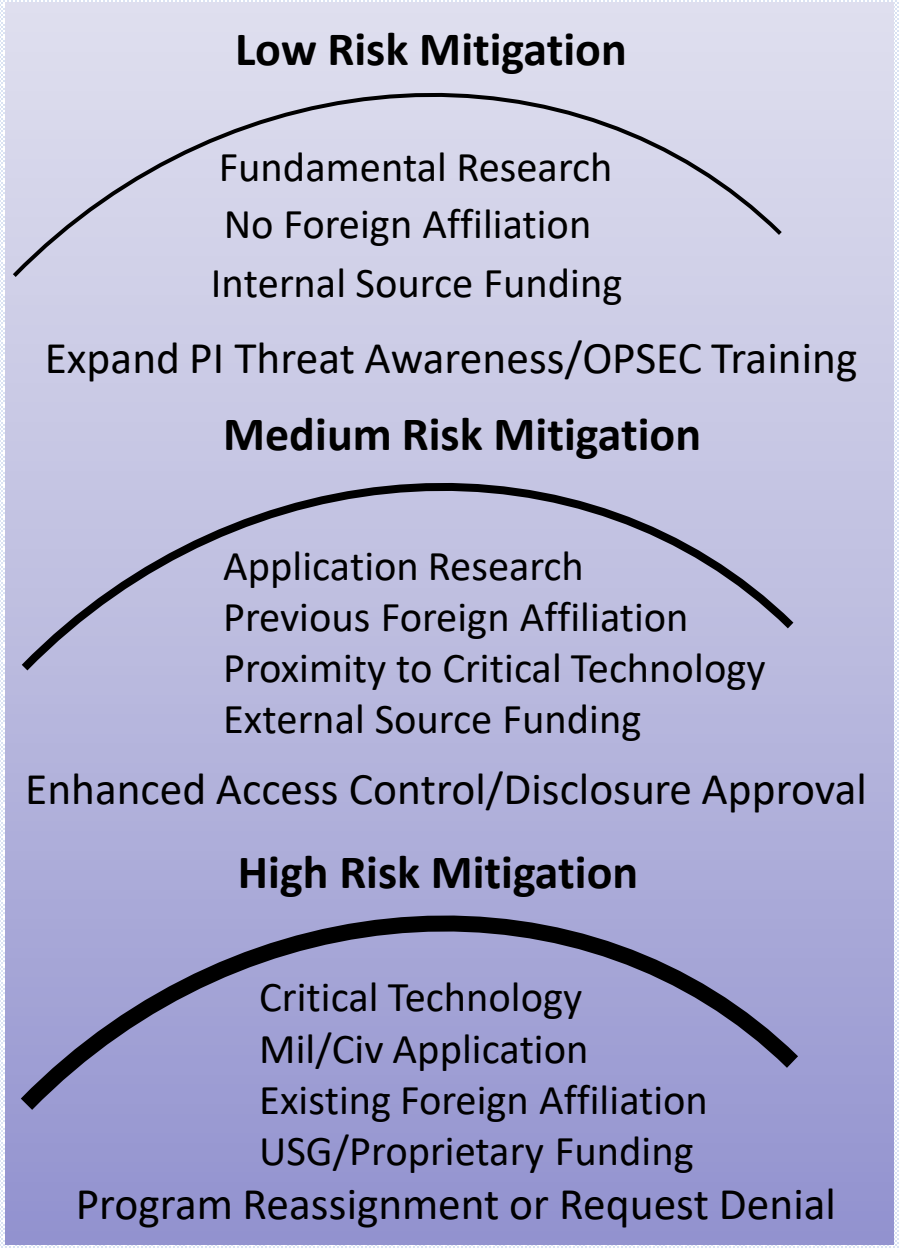
https://www.dni.gov/index.php/safeguarding-science

The NIST Research Security Framework



Framework Methodology – Starting with Yes

- **"It's About the Science" - Understanding the Science First**
  - PI awareness of U.S. technical art/parity of international science
  - Understanding the Why (intellectual property theft) is key to acceptance
  - Open communication fosters cultural acceptance and management buy-in
- **Implementation**
  - Collaborative Multi-disciplined Team Composition and Analysis
  - Use of Open-Source Tools and Federal Resources
  - Risk Analysis
    - **R**ecruitment, **A**ffiliations, **F**unding, and **T**echnology (**RAFT**)
    - Military-Civil Fusion Applications
- **Risk Mitigation**
  - Consensus determination with scalable non-intrusive countermeasures to mitigate levels of anticipated risk
- **Program Maintenance**
  - Recurring Case Review
  - Partnership Oversight



Review Fundamentals – Funding Opportunities

Funding Opportunities

- Contracts
- Grants/SBIR/ Incentives
- CRADAs
- OTAs

Reviews

- NSPM-33 applies to all recipients of more than $50M Federal R&D funds/year
- CHIPS & Science Act is bifurcated – incentives and R&D – same process
- SBIR/STTR Due Diligence

Risk Determination

- Composite Analysis of collected information
- Risk-balanced determination – ***Does the Benefit Outweigh the Risk ?***

Key Questions

Requestor supplied

- Organization
- Requestor (e.g., PI)
- Associates of requestor
- Technology type
- Export control
- IT security
- Patentable outcomes
- Military-civil fusion applications
- Financial
  - Ownership
  - Subsidiary ties
  - Partnerships and affiliations
  - Obligations (e.g., loans, venture capital)

Review Fundamentals – Foreign Collaborations

Foreign Collaborations

- Engagement
- Publications

Reviews

- Statutory requirements (e.g., covered individual, country of concern, etc.)
- All collaborations (initial contact request) and publication(s) (outcome) with country of concern organization (s) and authors are reviewed

Risk Determination

- Composite Analysis of collected information
- Risk-balanced determination – ***Does the Benefit Outweigh the Risk ?***

Key Questions

Requestor supplied

- Collaboration participants
- Technology type
- Benefit statement
- Export Control / Technology Control Plan
- Military-Civil Fusion applications
- Patentable outcomes
- Research funding source
- Publications

Review Fundamentals – Associate Appointments

Associate Appointments

- Foreign
- Domestic

Reviews

All associates are reviewed at least once per year

- Researchers, Contractors, Facility Users, Offsite Collaborators

Risk Determination

- Composite Analysis of collected information
- Risk-balanced determination – ***Does the Benefit Outweigh the Risk ?***

Key Questions

Associate supplied

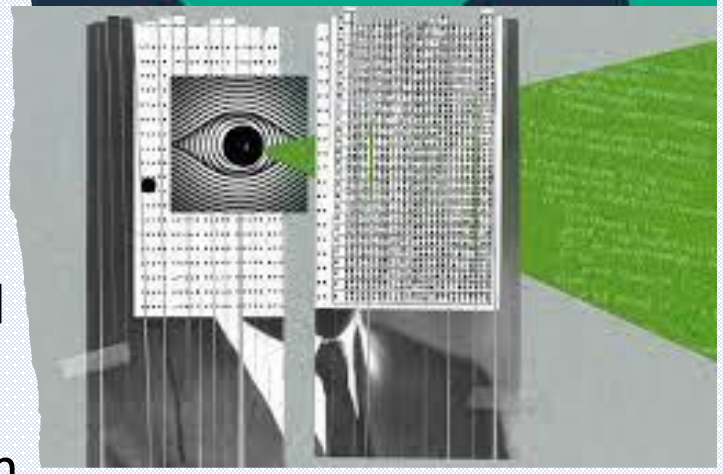
- Associate affiliations
- Legal status (Visa)

Organization supplied

- Host/Sponsor affiliations
- Method of recruitment
- Funding source
- Technology type
- Project plan
- Benefits to an organization
- Fundamental research plan
- Military-civil fusion applications
- Export control/Technology control plan
- Patentable outcome potential
- Federal initiative funding (e.g., CHIPS)
- Access control (logical and physical)

Risk to U.S. Research Community

- The binary Cold War nature of spying and foreign espionage is gone.
  - Expanding number of foreign (state & non-state) competitors
  - Diverse collection strategy and methods
  - Classified information no longer the primary target
  - ***Unclassified proprietary information and intellectual property may hold the keys to national dominance***
- Competitor nations apply whole of government tools to acquire or divert emerging technologies – through legal and illicit means – to achieve national military and economic superiority
- China, Russia, and Iran stand out as the three most capable actors tied to economic espionage and the theft of U.S. intellectual property
- Non-traditional information collection methods such as Malign Foreign Talent Recruitment or Placement programs facilitate the transfer of intellectual property from U.S. universities and research centers



The Non-Traditional Information Collector

A non-career intelligence asset who seeks to collect technical data and intellectual property on behalf of competitor nations or other foreign entities

- Collection Methods:
  - Cyber & Social Media Deception
  - Foreign Student/Scientist Exchange Programs
  - Professional Conferences
  - Malign Foreign Talent Recruitment and Placement Programs
- Motivations:
  - National Ideology or Strategy
  - Grants, Awards, Scholarships

An Emerging Challenge: Are NSDD–189 and NSPM-33 in conflict ?

"No restriction may be placed upon the conduct or reporting of federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes." NSDD-189

Points for Consideration:

- Modern technology collection methods are increasingly effective and pervasive
- Fundamental research and intellectual property are targeted to advance military/civil fusion strategies
- Competitor nations are employing non-traditional information collectors in collaborative research
- Some competitor nations are not like minded and don't share mutual objectives

Is the exchange of fundamental and applied research as benign today as it was in 1985 ?

Is NSDD-189 an entitlement to perform collaborative research that can benefit a competitor nation?

- Balkanizing federally funded fundamental research conduct and reporting could adversely affect U.S. R&D leadership
- The Research Security Framework complements NSDD-189 and NSPM-33 protections while meeting the requirements of new U.S. Statues (e.g., CHIPS & Science Act)

Framework Test Case – Quantum Physics

NIST researcher / U.S. University adjunct professor receives global requests to collaboratively develop the next-generation quantum system theories that solve QIS problems

- **Research Security Review outcomes:**
  - **Recruitment** – Request by Chinese graduate student asking to come to perform collaborative research
  - **Affiliations** – Graduate student at a Chinese Seven Sons of Defense University
  - **Funding** – Pre-funded by a Chinese Award (an identified malign foreign talent placement program) – PLA funding
  - **Technology** – Research scope assessed as U.S. emergent technology match to a PLA identified collection priority
- **What's at risk?**
  - NIST researcher's intellectual property and other contiguous research
  - U.S. research ecosystem and potential contribution to QIS mil/civ fusion objectives of the PRC
- **Risk Determination**
  - High
  - Potential Non-traditional information collector
  - While NIST researcher claims his research is purely fundamental and has no applications or intellectual property concerns, he recognizes the potential risk to NIST and the U.S. research ecosystem
  - His management concurs with recommendation to deny proposed collaboration

Questions and Answers

Safeguarding International Science

Achieve a balance between open scientific collaboration and research security that values collaboration while protecting U.S. intellectual property

researchsecurity@nist.gov

In person (Teams) review observations available on request

NIST Internal Report
NIST IR 8484

Safeguarding International Science

Research Security Framework

Gregory F. Strouse
Office of the Associate Director for Laboratory Programs
Laboratory Programs

Philip A. Bennett
Research and Technology Protection
Commerce Office of Security

Timothy R. Wood
Research Protections Office
Laboratory Programs

Mary Bedner
CHIPS Research and Development Program
CHIPS Program Office

Claire M. Saundry
International and Academics Affairs Office
Director's Office

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8484

August 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

https://doi.org/10.6028/NIST.IR.8484