NIST Internal Report
NIST IR 8484r1

Safeguarding International Science

Research Security Framework

Gregory F. Strouse
Timothy R. Wood
Claire M. Saundry
Philip A. Bennett
Mary Bedner
Jeremy F. Schultz

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8484r1

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8484r1

Safeguarding International Science

Research Security Framework

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

Timothy R. Wood*
Research Protections Office
Laboratory Programs

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

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

Mary Bedner
CHIPS Research and Development Office

Jeremy F. Schultz
International and Academic Affairs Office
Director's Office

** Retired*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8484r1

November 2025

U.S. Department of Commerce
Howard W. Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Publication History
Approved by the NIST Editorial Review Board on 2025-11-17
Supersedes NIST Internal Report 8484 (August 2023) DOI: 10.6028/NIST.IR.8484

How to Cite this NIST Technical Series Publication
Strouse G.F. et al. (2025) Safeguarding International Science Research Security Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8484r1.
https://doi.org/10.6028/NIST.IR.8484r1

NIST Author ORCID iDs
Gregory F. Strouse: 0009-0003-6462-6846
Claire M. Saundry: 0009-0003-4711-7177
Timothy R. Wood: 0009-0002-6098-5852
Philip A. Bennett: 0009-0003-4205-7689
Mary Bedner: 0000-0002-2183-7008
Jeremy F. Schultz: 0000-0003-2231-6797

Contact Information
researchsecurity@nist.gov

Abstract

This publication supersedes National Institute of Standards and Technology (NIST) Internal Report (IR) 8484 and adds a Research Security Risk Determination Matrix along with a discussion in Chapter 9. The U.S. science and research ecosystem retains its leadership by actively engaging with the global community through the conduct of mutually beneficial collaborative research and the welcoming of international scientists. Coupled with that, the national and economic security of the United States depends on effective risk management practices for organizations that engage in international collaborative research to protect against undue foreign influence and interference.

The NIST Safeguarding Science Research Security Framework ("Framework") establishes guidance to assist the U.S. science and research community [e.g., U.S. Government (USG), academia, and industry] across the broad spectrum of international science and technology activities as well as Federal funding initiatives. This Framework is designed to 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.

This Framework is a living document and will continue to be updated and improved as its users provide feedback on the implementation of review procedures or to address new or emerging risks. This will ensure it meets the needs of research security practitioners in a dynamic and challenging environment of new threats, risks, and creative solutions.

Keywords

research security; research security risk determination matrix; framework; safeguarding international science; CHIPS and Science Act; NSM-10; NSPM-28; NSPM-33; SBA SBIR/STTR Due Diligence; risk-balanced; collaborations; foreign influence; export control; technology control plan.

Table of Contents

List of Tables

List of Figures

Acknowledgments

We acknowledge NIST research library staff Mylene Ouimette, Rachel Eck, and Briget Wynne for identifying additional research security resources that are provided in Appendix A of this report. We thank NIST reviewers Robert Ivester, James St. Pierre, Kevin Stine, Anne Andrews, Christopher Szakal, Katherine Sharpless, and Kevin Kimball for their professional input and guidance on improving this Framework. We recognize Eric Lin (former NIST ADLP), who provided the initial impetus and leadership. We acknowledge ODNI NCSC for external support and encouragement; especially Andy Campbell, Rebecca Morgan, Lisa Thayer, Robert Rohrer, and Edward You.

Author Contributions

Gregory F. Strouse: Conceptualization, Methodology, Writing – Original draft preparation; **Claire M. Saundry**: Writing – Original draft preparation; **Timothy R. Wood**: Writing – Original draft preparation; **Philip A. Bennett**: Writing – Original draft preparation; **Mary Bedner**: Writing – Reviewing and Editing; **Jeremy F. Schultz:** Writing – Reviewing and Editing.

Executive Summary

This publication supersedes National Institute of Standards and Technology (NIST) Internal Report (IR) 8484 and adds a Research Security Risk Determination Matrix along with a discussion in Chapter 9. The U.S. research ecosystem retains its leadership by actively engaging with the global community through the conduct of mutually beneficial joint research and the welcoming of international scientists. Coupled with that, the national and economic security of the United States depends on effective risk management practices for organizations that engage in international research collaborations. Establishing a Safeguarding International Science Research Security Program ("Program") through an implemented framework provides checks and safeguards at key steps in program development and implementation to help manage responsible international engagement. Absent an effective Program, organizations risk running afoul of U.S. laws and regulations, which may result in criminal, civil, or administrative enforcement actions against an agency, individual employees, and/or private contractors. Organizations must maximize the benefits of international efforts while ensuring that any risks are mitigated, and that relevant U.S. laws and regulations are followed.

To better address these risks, in January 2021 the Office of the President published a memorandum highlighting the need to strengthen research security across the U.S. research ecosystem [1]. The memorandum and supplementary guidance from the Office of Science and Technology Policy call for the development of best practices to help organizations manage research security risks [2].

The purpose of the NIST Safeguarding International Science Research Security Framework ("Framework") is to establish guidelines to assist the science and research community [e.g., U.S. Government (USG), academia, and industry] in addressing the OSTP memorandum recommendations across the broad portfolio of international engagement activities. Once implemented, the Framework enables an organization to mitigate security risks while enhancing the benefits of engaging with the best foreign talent available.

This Framework is distinct from the NIST Cybersecurity Framework but is complementary in its intent to protect critical and emerging technologies within the broader U.S. research ecosystem.

The Framework's methodology is designed to protect individual privacy and civil liberties while reviewing potential risks of engagement. It is designed to assist organizations, regardless of size or risk profile of activities, to apply the principles and best practices of a balanced-risk management approach to improving the security of international research.

This Framework is a living document and will continue to be updated and improved as its users provide feedback on implementation or to address emerging risks or review procedures. This will ensure it is meeting the needs of the owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

1. Scope

The Framework is designed to strike a balance between openness, scientific research security, and international collaboration. The Framework outlines methodologies and requirements for an integrated, mission-focused, risk-balanced approach for safeguarding international science and technology from undue foreign interference while protecting the openness and integrity of the U.S. research ecosystem. This Framework is distinct from the NIST Cybersecurity Framework but is complimentary in its intent to protect critical and emerging technologies within the broader U.S. research ecosystem.

The Framework design is holistic, scalable, and adaptable to meet the different mission needs of the science and research community (e.g., USG, academia, and industry) – collectively called organizations. This Framework is available to those organizations that engage in mutually beneficial joint research with international partners in the furtherance of both international science and the best interests of the United States.

2. Background

This Framework was developed to integrate multiple USG policy and guidance documents to form a set of recommended security best practices. This approach fosters mutually beneficial international engagement while employing a risk-balanced methodology to safeguard U.S. scientific research and intellectual property from undue foreign interference while protecting the openness and integrity of our innovation ecosystem.

In January 2021, National Security Presidential Memorandum 33 (NSPM-33) on United States Government-Supported Research and Development National Security Policy [1] and the National Science and Technology Council (NSTC) Joint Committee on the Research Environment (JCORE) subcommittee established national security policy for U.S. Government-supported research and development (R&D) [3]. Key features of the documents are described below.

NSPM-33 established a national security policy for U.S. Government-supported research and development (R&D) to "strengthen protections of United States Government-supported R&D against foreign government interference and exploitation" while "maintaining an open environment to foster research discoveries and innovation that benefit our nation and the world." NSPM-33 focuses on three areas: 1) disclosure policy; 2) oversight and enforcement; and 3) research security programs. NSPM-33 guiding principles were issued by the OSTP to 1) protect America's security and openness, 2) establish clear and uniform policies and processes, and 3) ensure policies do not fuel xenophobia or prejudice [1].

The JCORE Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise document [3] is intended to compliment NSPM-33 and offers guidance for establishing a research security and integrity program within an organization. Encompassing a risk-balanced approach, the JCORE document focuses on five objectives: 1) demonstrate organizational leadership and oversight; 2) establish an expectation of openness and transparency: 3) provide and share training, support, and information; 4) ensure effective mechanisms for compliance with organizational policies; and 5) manage potential risks associated with collaborations and data.

In addition to NSPM-33 and the JCORE recommended practices, National Security Presidential Memorandum (NSPM-28) Operations Security (OPSEC) [4] and the Office of the Director of National Intelligence (ODNI) Safeguarding Science Toolkit [5] are the guiding documents used to create this Framework.

The NSPM-28 OPSEC cycle can be used as a mission-focused research security starting point to determine what intellectual property and technologies are at risk by foreign adversaries seeking to fill a technology knowledge gap using military-civil collection applications. The NSPM-28 OPSEC Program strategy is a fundamental construct of a successful research security program whereby the basic principles of the OPSEC process/cycle help determine critical assets needing protection and reinforce the safeguarding science objectives of any research security program.

The ODNI Safeguarding Science Toolkit is designed to raise awareness of the spectrum of risk in emerging technologies to assist stakeholders in these fields to develop their own methods to protect research and innovation. The four goals are to: 1) promote a U.S. research ecosystem, provide curated resources for our stakeholders, 2) support best practices in protecting research and innovation, assist academia and industry in developing their own methods, 3) protect intellectual property, and 4) foster information exchanges to better identify emerging-technology security challenges.

The Framework describes a set of methodologies to review various modes of international engagement and to make risk-balanced decisions. It is more accurately characterized as a security review process rather than an investigative instrument. However, it is recognized that in many instances mandatory background investigations for determinations of access to federal facilities and resources can supplement the Framework process [see Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12) [6]]. Conducting reviews prior to any background investigation can be cost effective and may lend itself to cultural buy-in of the research community.

Not unique to the Department of Commerce (DOC), many institutions both public and private have existing best practice programs in place upon which research security initiatives in response to NSPM-33 are based. Examples are provided in Appendix A: Additional Research Security Resources. As a precursor to NSPM-33, the DOC Administrative Order, DAO 207-12, “Foreign Access Management Program” established DOC policies and procedures for foreign national visitor and long-term guest access to Department facilities, resources, and activities [7]. This underlying policy recognizes the value of international contributions to U.S. science and research efforts and creates a baseline risk management program to ensure the benefits of international collaboration remain consistent with the strategic objectives of NIST and the DOC.

NIST has an established history of evaluating potential risks to its portfolio of international activities. In response to NSPM-33, the NIST Associate Director for Laboratory Programs (ADLP) ordered the creation of the NIST Scientific Research Security Team (“Team”) to develop an integrated approach to meet the guidance of JCORE, the requirements of NSPM-33, and DOC DAO 207-12. The Team established risk-balanced review methodologies across intramural and extramural programs and developed internal policies, protocols, and procedures to safeguard scientific resources and limit potential risk exposures to intellectual property theft. The Team also developed and implemented training and created necessary partnerships with intelligence, law enforcement, and non-Title 50 (NT-50) agencies of the federal government, academia, and industry.

3. Guiding Principles

3.1. Safeguarding International Science

The scientific research community recognizes that a diversity of perspectives accelerates scientific and engineering discoveries, as well as advances emerging technologies. The United States benefits from the talent of individuals from around the world, and we value that engagement. This Framework is designed to enable collaborative international research that fosters innovation, enhances U.S. scientific leadership, advances U.S. economic competitiveness and national security, and builds and maintains the relationships necessary to address a multitude of global challenges while managing potential risks to intellectual property and scientific integrity.

Advantages of supporting mission-focused international science include:

- Enables cutting-edge research that no nation could achieve alone
- Strengthens scientific and diplomatic relations
- Trains a robust science and technology workforce capable of solving global problems
- Significantly contributes to the research science ecosystem
- Enables international research that advances U.S. competitiveness in the global marketplace
- Promotes industry standards and regulatory regimes that harmonize the global economy
- Supports USG priorities and foreign policy objectives.

Conversely, overly restrictive research security policies can reduce U.S.:

- Leadership in research
- Influence in research objectives
- Development of industry standards
- Industrial competitiveness.

3.2. Organizational Core Values

The Framework methodologies are based on an organization's core values. For NIST, the core values are perseverance, integrity, and excellence [8]. The use of other guiding principles that are tied to an organization's mission-specific objectives are acknowledged and encouraged. It is critical that an organization's Research Security Team establish transparent guiding principles for staff to understand. Brief descriptions of NIST's core values follow.

- *Perseverance*: We take the long view, planning the future with scientific knowledge and imagination to ensure continued impact and relevance for our stakeholders.
- *Integrity*: We are ethical, honest, independent, and provide an objective perspective.

- *Excellence*: We apply rigor and critical thinking to achieve world-class results and continuous improvement in everything we do.

3.3. Understanding the Why

At NIST, the "Understanding the Why" message is based on the mission of NIST – To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life [8].

The era of binary Cold War spying has fundamentally changed. The traditional contest emphasizing the acquisition of national security secrets has increasingly been replaced by foreign economic and industrial espionage. Competitor countries seek to gain technical advantages through the theft of intellectual property that cuts across the three risk concentrations of national security, economic security, and intellectual property security. It is recognized that the number of foreign competitors is expanding with an increasing focus on fundamental science and research outcomes as the primary target to achieve national and military superiority. Through focused programs that implement new intelligence, surveillance, and reconnaissance capabilities, competitor countries are targeting unclassified proprietary information and intellectual property that may hold the keys to national dominance. Competitor nations apply whole of government tools to acquire or divert advanced technologies – through legal and illicit means – to achieve national military and economic superiority.

At the time of publication, China, Russia, and Iran stand out as the three most capable actors tied to economic espionage and the potential theft of U.S. trade secrets and intellectual property.

To be successful, a research security program must influence the culture at the institution. This can be achieved by focusing on safeguarding science rather than on security compliance. Establishing a partnership with the scientific and research community garners confidence that the program is "science centric" and that the application of scalable, non-intrusive countermeasures to protect intellectual property is a highly effective means to safeguard international engagement.

Cultural acceptance starts with open communication with staff and foreign collaborators acknowledging that international science enables cutting-edge research, and that the organization greatly values the contributions of its international partners. The Framework is designed to protect an organization's research from undue foreign threats or influence and preserve international engagement by striking a balance between security and the openness of the U.S. innovation ecosystem. This Framework may be applied to a global community as well. This balanced approach resonates with the scientific research community.

4. Goal and Overview

This Framework establishes a uniform research security implementation methodology designed to safeguard America's science and research community from undue foreign interference while safeguarding the benefits of international science, thus ensuring the integrity of the U.S. innovation ecosystem. The subsections below describe the objectives, implementation requirements, review portfolio scope, and key features of the Framework.

4.1. Objectives

There are three major objectives of the research security program:

- Maintain an inclusive culture that promotes international collaborative science while safeguarding the U.S. research enterprise.
- Develop and implement a strategic communication plan; provide regular input to organizational leadership.
- Develop and implement Safeguarding International Science research security policies, orders, and guidelines that align with U.S. national-level research security policy requirements and are tailored to facilitate organizational mission success.

4.2. Implementation Requirements

The requirements for implementing a successful research security program are provided below. Implementation of each requirement as it is applied to the research security review categories is described in more detail in Section 7.

- Conduct an assessment to identify critical assets (e.g., intellectual property and technologies), consider foreign adversarial threats, identify vulnerabilities and risk of exploitation, and develop countermeasures to mitigate risk of intellectual property theft (see NSPM-28 OPSEC Cycle).
- Conduct an analysis to identify where and how implementing research security guidance intersects with organizational business processes.
- Design effective and efficient research security protocols that complement existing business processes to advance organizational mission success and safeguard international science initiatives.
- Conduct tailored reviews of international science programs and activities to reach informed risk-balanced access determinations consistent with mission objectives.
- Provide organizational guidance and assistance on methods to safeguard international science by establishing mechanisms for regular discussion of current threats, risks, vulnerabilities, and other relevant research security issues impacting science and research programs.
- Develop and provide research security awareness training, tools, and resources

for standard application across the organization.

- Provide a forum to discuss and evaluate research security best practices and their contribution towards organizational mission success.
- Partner with internal organization departments with specific expertise (e.g., Export Compliance, Grants, Publication Clearance, Human Resources, Information Systems (cybersecurity), Insider Threat, Physical Security, Public and/or International Affairs, General Counsel, etc.) to serve as ad hoc team members, increase awareness, and enhance cultural integration.
- Partner with external organizations (e.g., U.S. intelligence community, law enforcement, USG agencies, academia, industry, and international partner organizations) to create a venue for awareness and feedback.

4.3. Key Framework Elements and Characteristics

A list of the major program elements for establishing a successful research security program is provided below. Each element is described in more detail in the subsequent sections as listed below.

- Multi-disciplinary research security team
- Strategic communication and organizational integration
- Mission-focused review portfolio and methods
- Integrated risk-balanced methodology and determination
- Export control, Technology Control Plans, and compliance procedures

In addition to the major program elements, a research security program must have the following characteristics to ensure successful adoption across the organization.

- *Transparent methodology* so the staff understand the overall program and the methods of implementation. It is important to use effective communication and training so that staff culturally accept and positively integrate research security into their workstream rather than seeing research security implementation as an unknown burden and/or negative process. An informed workforce that understands “why” it is important and “how” research security works will understand the benefits of the program and actively participate.
- *Defensible policies and processes* that are mission-focused, non-invasive, and non-intrusive. These policies are the backbone of an effective research security program. They define the program, describe the transparent methodologies, and establish organizational authorities. The policies and processes should be developed and implemented to create a defensible program such that they can be audited by an outside agency (e.g., GAO).

Combining the key Framework elements and characteristics above enables the creation of an integrated research security platform that is driven by the organizational core mission science and technology competencies, as depicted in Figure 1. Communication and integration across an organization is the center point of obtaining staff awareness and involvement. One or both program types (e.g., extramural and intramural) may be applicable depending on the mission of the organization.

Extramural programs are those where an organization is creating a potential risk by projecting intellectual property outward (e.g., funding, publications, travel, and other research products).

Intramural programs are those where an organization is creating a potential risk by bringing foreign organizations or citizens into their working environment or allowing access to intramural research by other means. These risks are mitigated through the application of a case-by-case risk-balanced analysis, implementation of user activity monitoring (e.g., non-intrusive countermeasures), and well-informed staff (e.g., communication/training) who understand both the risks and the benefits of international science.

Figure 1. An overview of the key framework components that integrates and connects across the research security program.

5. Research Security Team

A multi-disciplinary Research Security Team is essential to the success of the Program. The Team develops and executes the research security framework within the organization. The following sections describe notional team composition, responsibilities, and meeting structure.

5.1. Composition and Expertise

Team membership should include a diversity of unique subject matter expertise/disciplines. Representation from mission-oriented components of the organization is key to ensuring cultural acceptance as well as understanding of both research security and operational objectives. This enables translation of research security information into mission objectives, creates an approachable team, and allows for an inclusive culture.

The team should include core and ad-hoc members. Core team members should be able to understand the mission-centric relationships between critical and emerging technologies, international science, and research security. The model and number of core team members depends on the size and mission of the organization and the scope of the programs to be reviewed. An example is a minimum team that contains expertise in research science (e.g., publishes scientific findings), export control, research and threat protection [(RTP) e.g., intelligence and counterintelligence], international engagement, IT security, and cybersecurity.

One example of a Research Security Team structure, with proposed roles and responsibilities, is outlined below. This model is adaptable to other patterns, but the reflection of organizational core mission competencies is essential to achieve success.

Mission Focus: Research Security Team Lead
Provides the requisite technical, scientific, and research experience and expertise to effectively evaluate the scope, credibility, and benefit of proposed foreign collaboration as a principal consideration of the risk management analysis. The team lead is responsible for facilitating discussions on research security protocols, recommending training initiatives, and leading interagency engagement and collaboration. The team lead makes the risk management determinations based on recommendations from the team. The team lead should be appointed by the organizational Director.

International Focus: International Affairs Manager
Provides the requisite international program and foreign affairs expertise to effectively evaluate the applicability and scope of international, academic, or interagency exchange agreements, the benefit of proposed foreign collaboration, and the potential international science and technology policy implications as a principal consideration of the risk/benefit analysis.

Export Control Focus: Export Control Manager
Provides the requisite U.S. export control expertise to effectively evaluate the

applicability and extent of U.S. export licensing or disclosure requirements associated with any anticipated transfer of U.S. technology, technical data, commodity, or software associated with the proposed foreign collaboration as a principal consideration of the risk/benefit analysis.

IT Security Focus: Information Security Officer
Provides the IT security, requisite federal cybersecurity, information technology, and systems expertise to effectively evaluate the scope of information system access, vulnerabilities, and overall system integrity associated with the proposed foreign collaboration as a principal consideration of the risk/benefit analysis.

Office of Security: Research and Technology Protection (RTP) Officer
Provides the requisite security, intelligence, counterintelligence, RTP, OPSEC, and risk management expertise to effectively evaluate the potential foreign collection threat associated with the proposed foreign collaboration as a principal consideration of the risk/benefit analysis.

Ad-hoc Team members may include representatives from legal counsel, mission-focused programs (e.g., organizational leadership), physical security, insider threat, grants, publication review, technology transfer, the intelligence community, or other subject matter experts to address specific issues.

5.2. Official Reporting Structure

A hierarchal reporting structure must be established to ensure program awareness and provide recommendations to organization leadership and staff. For example, at NIST the team lead reports to the Principal Associate Director on a biweekly basis or as needed with recommendations around action items, outreach to the intelligence community (IC), and mitigation strategies on potential risks to the scientific mission. Awareness discussions may include upcoming training and new initiatives. This enables organizational transparency as well as a mechanism for an appeal of a non-concurrence finding, or decisional input (e.g., outreach to the intelligence community). Biweekly reports allow for discussions on current and upcoming reviews (see Section 7), training initiatives, external outreach (e.g., IC), new review initiatives to meet changing requirements (e.g., new USG initiative), and awareness of any potential concerns that may impact the organization's scientific and technology mission.

5.3. Administrative Responsibilities

In accordance with the goals and objectives above, the team is responsible for providing guidance and oversight on recommendations for new, or modifications to existing, policies, practices, procedures, technology applications, and/or funding pertinent to and in support of the Safeguarding International Science Research Security Framework.

5.4. Meeting Structure

Frequency
The team should meet at least once every two weeks to conduct team business or perform necessary reviews (see Section 7).

Agendas
The team lead should determine the agenda for all meetings with input from the membership.

5.5. Subcommittees and Working Groups

The team lead may establish and dissolve subcommittees and working groups when deemed necessary for the team to advance its goals and objectives (e.g., develop a new review process for use within the organization, develop new training material, assemble subject matter expertise for a specific review). Governing guidance should be provided to the subcommittee/working group at the time of creation. All subcommittees and working groups should be chaired by a permanent member of the research security team. Final reports, with findings and recommendations, should be presented to the team for further action.

6. Communication and Integration

At the core of Framework implementation is communication and integration throughout the organization. Strategic communication is key to explaining the "Why" to staff on the importance of integrating a safeguarding international science program. Table 1 gives a nominal list of strategic communication components to enact. Descriptions of each of the components follow.

Table 1. Communication strategy components.

Internal Communication
Key Staff Engagement
Management Support
Training
Open-office Hours
Centralized Email
Documented Policies and Processes
Internal Website

Internal Communication
It is important that information about the Program be communicated effectively throughout the organization for awareness and compliance. Internal tools may include communication through administrative fora, all-staff emails, in-house newsletters, town hall meetings, a centralized internal website with Program and contact information, etc.

Key Staff Engagement
It is important that Program information and requirements are disseminated to all staff who engage in activities covered by the program or who provide administrative support for such activities. Recruiting key staff to serve as messengers of the importance and benefits may attenuate staff resistance to change. Selecting well-known and in some cases world-renowned staff members to be vocal advocates helps set a positive organizational tone.

Management Support
The implementation of any new program within an organization requires management support to ensure its long-term success. It is important for management to understand the value proposition and opportunity afforded by establishing an organizational research security program. It is equally important for management to not inadvertently undermine the program by representing it as administrative burden or a 'check-the-box' exercise. Management is required to be part of the review process to show their support as well as to provide a balanced perspective in the process.

Training
Staff who are engaged in or support activities covered by the Program must be trained across a set of organizational requirements (e.g., IT security, safety, physical security, foreign travel) on a periodic and recurring basis. Additionally, the Research Security Team provides specific

training for safeguarding international science that is modified to meet the organizational mission (e.g., counterintelligence, operations security). As a minimum, yearly research security training that covers staff responsibilities (as determined by an organization), changes to the threat environment, counterintelligence, operations security, foreign interference or influence directed against the U.S. academic and research community, and responsibilities should occur. Program-specific training is necessary as well. For example, if an organization hosts foreign nationals, then an annual training brief should be given to the sponsors hosting those foreign nationals, as well as any staff serving as escorts to foreign national visitors (This includes day visits and longer.). Quarterly updates may be used to cover situational changes (e.g., new risk, new research security review), provide awareness, and reinforce cultural buy-in as well as providing staff a communication feedback mechanism.

Open-Office Hours
It is important to establish an informal mechanism that enables staff to ask questions about the Program, suggest changes, and give quick updates. Often staff bring up a concern that may also impact others – this helps prevent siloed thinking. For example, the team could establish and hold regular office hours as one possible mechanism or host lunch-and-learn or coffee-hour sessions (in-person or virtual).

Centralized Email
A centralized, easy to remember email alias for contacting the team with questions and comments should be established for both internal and external communications related to research security. This enables the appropriate team member to respond to the inquiry and for all team members to be aware of the inquiries and concerns and to standardize responses.

Documented Policies and Processes
Once research security processes and policies are developed within an organization, they should be documented for awareness, consistency, training, and transparency. The documents should also be used to communicate the research security program and should be shared widely and made easily accessible across the organization.

Internal Website
If applicable, the organization should consider developing and maintaining an internal website to serve as a hub for information related to the research security program, including the documentation mentioned above.

7. Mission-Focused Reviews: Methodology and Categories

A rigorous research security review process and approval methodology are integral to the Framework and provide mechanisms to protect the research and to identify and limit potential organizational risk exposure.

As shown in Table 2, reviews are broken into several main categories and represent the associations and activities that are important to the organizational research mission and are within the purview of the research security program. This portfolio may not represent all possible associations and activities and should be tailored to meet the needs of the organization. Additionally, the review portfolio is expected to be dynamic and should be updated as the needs of the organization change. Descriptions of the review categories and more details on conducting the reviews are provided in the subsequent subsections.

Table 2. Main review categories for safeguarding the security of international science.

Review Category	Subsection	Potential Scope (Non-Inclusive)
Research Associate Appointments	7.1	• Foreign national associates • Domestic associates
Foreign Travel Requests	7.2	• Virtual and in-person foreign meetings and visits • Assistance in kind from foreign sources
Foreign Collaborations	7.3	• Research publications with foreign coauthors • Engagement with foreign collaborators
Foreign Request for Products, Services, and Software Tools	7.4	• Products produced and sold • Services provided • Databases (free) • Online research tools
Extramural Funding Opportunities	7.5	• Contracts • Grants • Cooperative research and development agreements (CRADAs) • Grand Challenges and prize competitions • Other transaction authority (OTA) agreements

A review of any type is comprised of several basic components. Table 3 gives a nominal list of the review methodology components necessary for a research security team review.

Table 3. Review methodology components.

Identify Review Need
Information Collection
Review and Composite Analysis
Risk Determination
Recommendation
Long-Term Maintenance and Countermeasure Assignment
Country of Concern and/or Critical and Emerging Technology
Forms
Open-Source Intelligence (OSINT)
Consensus and Legal Authority
Concur, Concur with Provisos, and Non-Concur
Continuous Monitoring

Figure 2 shows the three main pillars necessary to implement a research security review process for the five main review categories (listed in Table 2): from the start (e.g., information collection), the risk-balanced composite analysis and recommendation, and monitoring that follows a review and positive decision.

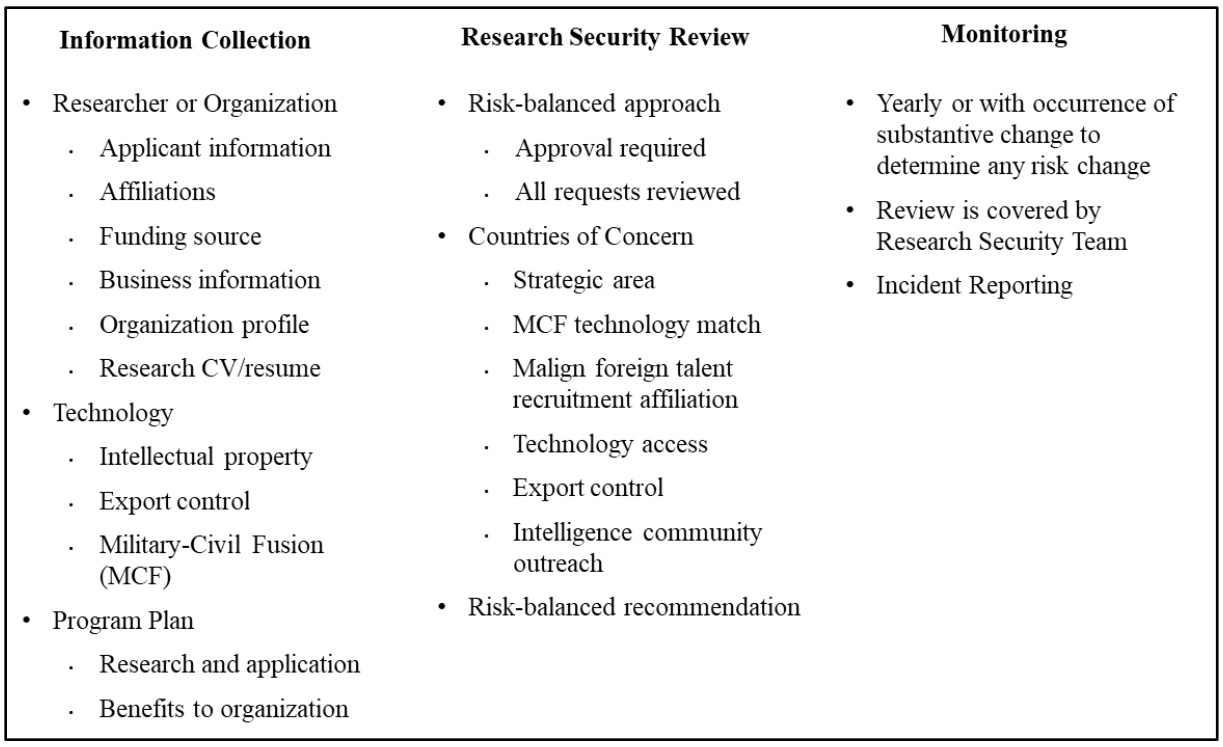

Figure 2. Review methodology implementation pillars for the five review categories

The following sections are intended to stand alone and present nominal processes for the five different research security review categories: 1) Research Associate Appointments, 2) Foreign

Travel Requests, 3) Foreign Collaborations, 4) Foreign Requests for Products and Services, and 5) Extramural Funding Opportunities. It is expected that an organization may adapt the described research security review category methodologies to meet their own organization structure and mission.

7.1. Review Category 1: Research Associate Appointments

This review category applies to research associate appointments within the organization (both physical and remote or virtual). Research associates generally fall into two categories: foreign associates and domestic associates. A foreign national associate (FNA) is any individual working within the organization who is not a United States Citizen [e.g., foreign citizenship or U.S. Lawful Permanent Resident [(LPR) *aka* Green Card Holder] or permanent employee. FNAs can range from guest researchers working in the labs to contractors performing support services. A domestic associate is any individual working within the organization who is a U.S. citizen but is not a permanent employee. Domestic associates can range from guest researchers working in the labs to contractors performing support services. While this Framework is focused primarily on foreign influence and interference by non-U.S. citizens (and organizations), the review methodology may be applied to domestic associate appointments.

The Research Associate Appointment Review Form asks the key questions necessary to complete a review with the other information collected as supporting documentation (Appendix C). The various nominal sources used to collect information to populate the form are given in Table 4. It is recognized that a specific mission-focused version of the form may be required to meet the needs of the home organization. Some of the information collected may be used to initiate a background investigation as required by the organization (e.g., Human Resources, Physical Security, Insider Threat). A background investigation is usually outside the purview of a research security program.

The team considers not only the expertise and experience of the potential foreign-national researcher (associate) and their contributions to the institution's programs (the "benefits") but also when export-control concerns may exist or the potential for military/civilian fusion (MCF) technology applications as well as their institutional affiliations, funding sources, and scope of access to technology, equipment, and resources. As needed, the team meets with the hosting researcher and hosting technical leadership/management to discuss and review foreign-national researcher appointments.

For a new agreement, either a team document review or an in-person review is used. Associates from countries of concern, and others at the discretion of the team, will trigger an in-person review. In-person reviews require the attendance of the host/sponsor and their management and a majority of the core research security team members.

Table 4. Nominal information sources for an analysis of a proposed research associate appointment.

Research Security Form – Key Questions
DOC 207-12 Foreign National Request (Includes necessary information for background investigation)
Export Control / Technology Control Plan
Host/Sponsor Training Status
CV/resume – Education, Experience, Funding, Organizational Membership
Internet Search Engine, Persistent Digital Identifier
Potential Conflicts of Commitment and Interest

For a new agreement, a notification is sent to the sponsor via e-mail. An excerpt example of the text is given below:

> *This is a new agreement for (associate name inserted).*
>
> *New agreements and extensions for Foreign National Associates (FNAs) may trigger a review by the research security team.*
>
> *For New Agreements, if a review is required, the team will contact you to schedule a meeting with the FNA's Host, Division Chief, and the OU approving official.*

For extended agreements, within the one-year review interval, the sponsor must confirm that there have been no changes. An excerpt example of the text is given below:

> *For extensions, if the initial appointment for this FNA required a review with the research security team and that review was conducted in the past year, the team requests email confirmation (to researchsecurity@nist.gov) that there have been no substantive changes to the appointment (i.e., research plan, benefit, FNA employer/sponsor, funding source, NIST host, export or mil/civ applications, and access) since the previous review.*
>
> *We also request the Host to confirm that the FNA has made positive contributions to program/project objectives and that there has been full compliance with all NIST safety, security, and IT protocols consistent with the "Certification of Conditions and Responsibilities for a Foreign National Guest" (DAO 207-12, Foreign Access Management Program, Attachment 2).*

All associates are reviewed. Reviews must be performed at a minimum interval of one year or, in the interim if there are substantial changes (e.g., funding, sponsor, research effort, employer, and Visa status) to the answers to the key questions (7.1.1).

7.1.1. Key Questions

Answers to key questions are used during a review to determine whether the benefit of hosting an associate outweighs the potential risk. The answers are supplied by the host/sponsor and used to populate the Research Associate Appointment Review Form (Appendix C) prior to a review. A review reference guide for the key questions is found in the Research Associate Appointment Checklist (Appendix D).

The key question topics are listed below, followed by more detailed descriptions:

- Associate Affiliations
- Origin and Method of Recruitment
- Legal Status (Visa)
- Host/Sponsor Affiliations
- 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
- Congressional Requirements and Restrictions
- Access Control (Logical and Physical)

Associate Affiliations
Affiliations include any past or present organization (foreign and domestic) with whom the associate has a formal relationship or obligations (*e.g.,* universities, scholarships, professional societies, foreign talent recruitment programs). The nominal starting point is through a CV/resume and publications (e.g., internet search engine, persistent digital identifier). The associate may be directly (e.g., actively publishing or working for) or indirectly (e.g., undergraduate, or previous employer) affiliated with an organization. Indirect affiliations pose less risk and should be factored into the risk assessment accordingly.

The risk associated with an organization affiliation is dynamic and must be revisited annually. Risk-balanced adjudication is factored in multiple ways via the following method:

- Determine the risk level of the affiliated organization using OSINT resources (examples are given below)
    - Australian Strategic Policy Institute (ASPI) China Defense Universities Tracker
    - International Trade Administration Consolidated Screening List (ITA CSL)
- For a university, determine whether the person is or was an undergraduate or graduate student
    - A graduate student is most likely to be performing and publishing research that may be part of defense-related program at their university

    - Free OSINT tools (e.g., internet search engine, persistent digital identifier) should be used to determine if the associate is actively publishing through the university and/or if there is any foreign funding (e.g., scholarship, grants)
    - Country of concern affiliations, especially those determined to be one of the CCP/PLA Seven Sons of National Defense +One, require further investigation into activity (e.g., direct or indirect)
- For a foreign talent recruitment program, determination of whether the program is malign or benign is critical. Association with a malign foreign talent program is considered a very-high risk, and the risk will likely outweigh the benefit
- For a company, determine if there are any export control issues (e.g., ITA Consolidated Screening List)

Common Indicators and Warnings

- Seven Sons of National Defense affiliation and activity level
- ASPI High Risk or Very-High Risk identification
- Malign Foreign Talent Recruitment Program
- Foreign Funding
- Export Control

Resource Tools

- CV/resume
- Internet Search Engine
- Persistent Digital Identifiers
- Social Media
- Risk Level through ASPI
- Export Control through ITA Consolidated Screening List

Origin and Method of Recruitment

Understanding how the proposed associate was recruited is important in understanding whether this was an open competition, collegial association, or a direct/unsolicited contact. It is preferred that recruitment be an open competition. In the case of a recruitment via collegial association, the knowledge of the relationship and historical working involvement is discussed. Collegial recruitment may be an inherent risk if there is a constant flow of potential associates all from the same country of concern with past (e.g., undergraduate) affiliation with an organization of concern. Direct/unsolicited contact needs to be considered a potential phishing opportunity by a non-traditional collector of intellectual property. Scientific credibility must be determined to assess risk.

Common Indicators and Warnings

- Constant flow of collegial recruitment from one country of concern organization
- Direct contact
- University affiliation with a malign foreign talent recruitment program (e.g., Confucius Institute, Chinese Association for Science and Technology)

Resource Tools

- CV/resume
- Sponsor
- ASPI
- Center for Security and Emerging Technology (CSET)

Host/Sponsor Affiliations

Identifying affiliations is necessary for understanding whether there are any potential conflicts of interest or commitment. Additionally, this is useful for identifying attachments to malign foreign talent recruitment programs.

Common Indicators and Warnings

- Affiliations with country of concern organizations
- Funding from country of concern organizations
- Contracts or Memoranda with country of concern organizations

Resource Tools

- Host/Sponsor
- Internet Search Engine
- Persistent Digital Identifiers
- FNA Funding Source

Funding Source

The funding source must be determined. Funding for a proposed associate and a project may or may not be from the same source. Typical funding sources may include the home organization, other USG organizations [e.g., National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA)], a university, a commercial source, and a foreign scholarship. For other U.S. organizations (e.g., USG organization or commercial), it becomes paramount that the funding organization is informed and grants permission for the associate to work on the project. Certain foreign scholarships are malign and must be avoided – the most common one from a country of concern is the Chinese Scholarship Council [9].

Common Indicators and Warnings

- Foreign scholarship from a country of concern
- External U.S. funding (e.g., DARPA) focused research

Resource Tools

- CV/resume
- Internet Search Engine
- Persistent Digital Identifiers for publications
- Social Media
- Current and pending support information
- Risk level through ASPI
- Export control through ITA Consolidated Screening List

Technology Type
A determination should be made on whether the research is tied to the Critical Emerging Technology List and the scientific mission of the home organization (see Critical Emerging Technology List and the ODNI Safeguarding Science Toolkit).

Common Indicators and Warnings

- Technology match to ODNI-identified country of concern technology focus
- Technology match to ASPI-identified country of concern technology focus
- Export control of technology for specific organizations

Project Plan
The project plan is a short explanation of the statement of work. It is used as an overview of the research and identifies the technology. Additionally, determine if the proposed effort is fundamental or applied research.

Common Indicators and Warnings

- Country of concern interest in identified technology
- Standards development

Benefits to the hosting organization
The benefits of the engagement to a hosting organization must outweigh the risks. In this case, it is the benefit to the mission of the organization and not to the host/sponsor of the associate. This benefit is weighed against the risk of foreign access to the programmatic research. Understanding what the associate will do (as reflected in the project plan), how the proposed associate will contribute to the success of the research, and what the associate will have access to are key factors to consider. An associate may not be a Principal Investigator (PI) – creating an enhanced economic and/or national security risk.

Common Indicators and Warnings

- Associate will be or appears to be the PI
- Standards development
- Product and service engagement

Export Control / Technology Control Plan
Whether classified or unclassified, agencies possess information and technology that requires protection and/or review prior to its transfer. Such information includes export-controlled, proprietary, and other sensitive unclassified information that may be valuable and/or of interest to foreign governments or companies. The Technology Control Plan (TCP) must be approved by the designated export official to ensure compliance with U.S. law and regulatory requirements (e.g., EAR/ITAR).

Common Indicators and Warnings

- Scope of research
- Items, software, technology, etc. to be shared
- Research type
- Proprietary or public domain
- Foreign commercial availability

Resource Tools

- International Trade Administration Consolidated Screening List (ITA CSL)
- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Internet Search Engine

Fundamental Research Plan

Describe the fundamental research in terms of a publication abstract and clearly articulate that the research outcomes will be made publicly available.

Military-Civil Fusion

Military-Civil Fusion (MCF) is a national strategy through which select competitor nations pursue the collection of leading or emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitor nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by diverting leading-edge technologies through multiple venues such as cyber theft as well as open publications and international collaborative research, to accelerate the capability of their commercial and military/defense industries within the global economic environment.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies resident within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

Common Indications and Warnings of Foreign Collection Interest

- National strategies (MCF, etc.) targeting emerging technologies (e.g., artificial intelligence (AI), quantum, bio-economics, autonomous systems, semiconductors, etc.)
- Technology/knowledge gap of competitor nations (e.g., years ahead/behind)
- Competitor nation researchers seeking to collaborate on targeted or knowledge gap research
- Current or past affiliation of foreign researchers to competitor nation-sponsored academic or research institutions and foreign talent recruitment programs.

Resource Tools

- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Sponsoring Principal Investigator as the technology subject matter expert
- Senior technical advisors for implications of potential international collaboration (risk/benefit analysis)
- Malign Foreign Talent Recruitment Programs

Patentable Outcomes
This question is often used as a tangential question for Military-Civil applications as the query is directed to the possible commercial use of the technology in question. The researcher is likely more apt to consider patentable applications as a routine aspect of technical progress or maturation. If the PI can identify a possible patentable or commercial application near or at the conclusion of the research project, then there is reason to infer that a military-civil fusion application may also exist.

Ties to Congressional Requirements and Restrictions
Examples to consider are based on congressionally funded programs (e.g., CHIPS & Science Act) where research security requirements and restrictions are specifically identified.

Access Control
In the context of research security, access control generally fits into two categories: physical (access to facility, laboratory, or research space) and logical (access to information technology systems or the virtual environment). For further guidance on physical facility security see Interagency Security Committee Standard and for logical security see NIST Cybersecurity Suite.

Physical access control should be considered an essential research security component. While traditional lock- and key-systems often are a mainstay of access control, the use of electronic Physical Access Control Systems (PACS) or digital electronic lock systems are typically applied to control ingress to and egress from controlled laboratory or research spaces. Perimeter and point of entry controls provide for security in-depth but should also be scalable (e.g., employ use of video monitoring or closed-circuit TV) to address expanded levels of risk based on sensitivity of research, unique equipment or value, or the introduction of foreign national researchers as part of collaborative international science initiatives. Additional controls such as periods of access (e.g., business or security hours access) complement existing controls when supplemented by approval processes that require additional supporting documentation to permit expanded access. Moreover, across a programmatic research environment there may be many research projects working in parallel. Determinations of access to contiguous research project spaces should therefore be considered during the review process as expanded access may permit unauthorized access to third-party intellectual property or proprietary research.

If an organization is conducting background investigations or screening audits as part of its security program, the granting of access should only occur after a successful adjudication of the investigation or audit results.

Common Indicators and Warnings

- Unauthorized physical access to contiguous research projects or spaces
- Requests for physical access to laboratory or project space not related to their research
- Request for after business hours access that exceeds project scope or defined need-to-know

Resource Tools

- Physical Access Control System

- User Activity Monitoring

IT security and cybersecurity

An organization's research security program must integrate information technology (IT) security system elements, including cybersecurity. Implementing both cybersecurity and IT security best practices creates a risk-balanced approach to determine logical access to science and research information resources, as well as how and when that access is managed.

Examples of IT non-intrusive countermeasures include:

- Limit the use of personally owned devices on the host organization's network to internet use only with no connection to internal organization systems
- Monitor remote access to an organization's network [e.g., User Activity Monitoring (UAM)]
- Recognize the sensitivity of data and restrict proprietary information to authorized networks and personnel only
- Meet IT-applicable export control requirements (EAR)

Common Indicators and Warnings

- Attempted unauthorized access to contiguous research projects
- Requests to access research project space not related to their research
- Requests for elevated privileges

Resource Tool

- NIST Cybersecurity suite of standards, guidelines, and resources
    - IT Access Control System
    - Network Connectivity and Access Monitoring
    - User Activity Monitoring

Travel

Situational awareness of an associate's travel plans may identify a non-traditional collector of intellectual property from an organization. Report of travel is managed through a travel request to the Team – See the Foreign Travel Review Form in Appendix C.

Common Indicators and Warnings

- Location and purpose of travel
- Unauthorized use of communication devices (e.g., phone, laptop)
- Research topic area (e.g., critical and emerging technology) for official travel

Resource Tools

- Travel request form
- IT user activity monitoring

7.1.2. Review Process

The following figure provides a high-level overview of the research security review process for associate appointments, including the risk determination and recommendations (described in more detail in the subsequent Section 8).

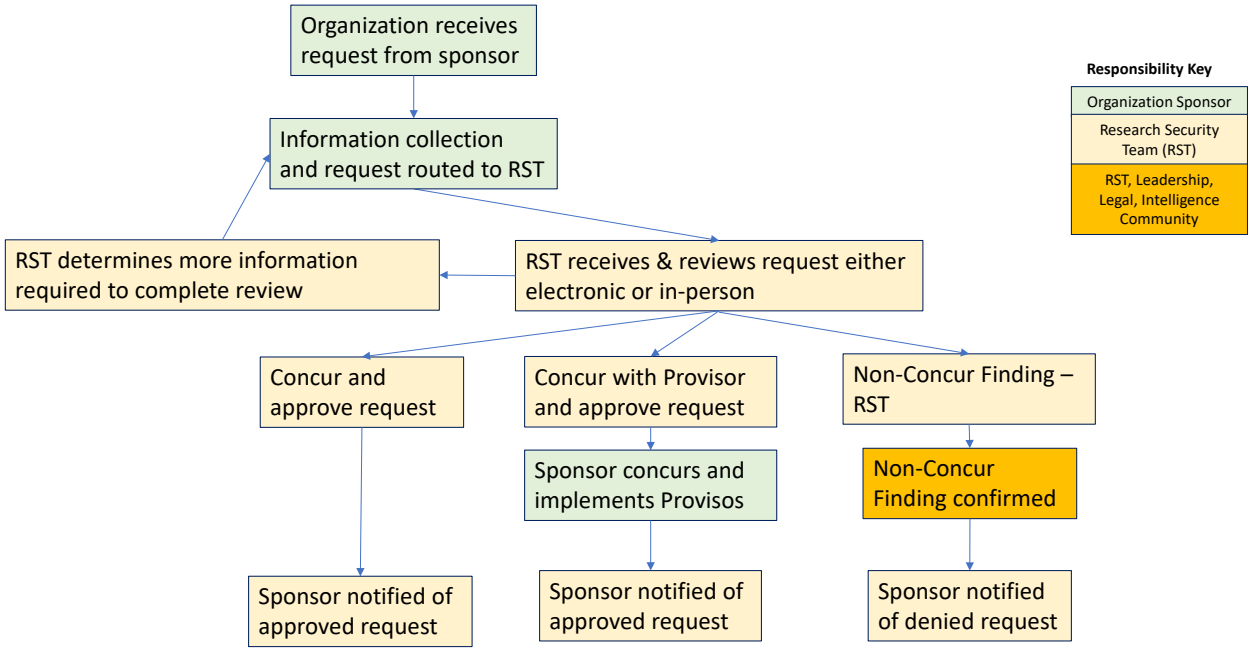

Figure 3. Research security review process for research associate appointments.

7.2. Review Category 2: Foreign Travel Requests

Foreign travel can be requested by either staff or associates and may be of two types – physical or virtual. Both types require review based on travel-to location, reason for travel, and host of event.

7.2.1. Key Questions

Key questions are used to determine whether the benefit of travel outweighs the potential risk. The Foreign Travel Request Form (Appendix C) is used to submit a travel request for review. A review reference guide for the key questions is found in the Foreign Travel Checklist (Appendix D).

The key question topics are listed below, followed by more detailed descriptions:

- Name of traveler
- Type of travel
- Event type
- Purpose statement
- Title and Abstract (for speakers)
- Name of event and event website information
- Event host organization(s)
- Benefit statement
- Foreign funding support / Assistance in kind (AIK)
- Military-civil fusion applications
- Research funding source

Requestor with organizational structure
The name of the travel requestor and their location within the organization.

Type of travel
Travel can be physical or virtual. While there are similarities to both types of travel, there are distinct differences that must be considered. Physical travel to a State Department designated Level 3 or higher location/country [10] must be discussed with the requestor and their management regarding personal safety considerations. Virtual travel concerns must consider the unknowns (e.g., who is attending).

Common Indicators and Warnings

- Invitation from an organization in or affiliated with a country of concern
- Physical travel to a State Department Level 3 or higher location
- Unknown attendees in a virtual travel environment

Resource Tools

- State Department Travel Advisories

Event type
Identification of the event type (e.g., International Conference/Workshop/ Standards Meeting/Collaboration/Presentation/ Other) is important in understanding the type of request (e.g., audience is by invitation only or public).

Common Indicators and Warnings

- Invitation from an organization in or affiliated with a country of concern

Resource Tools

- Travel request form
- Offers of AIK or reimbursement for expenses

Purpose Statement
The requestor should identify the reason for attending the event.

Common Indicators and Warnings
- Reason is tied to a critical emerging technology and the event is located in or sponsored by a country of concern

Resource Tools
- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Export control of technology for specific organizations

Title and Abstract (for speakers)
Title of talk and submitted abstract for the event are reviewed to better understand whether the technology being presented is a critical and emerging technology, new or already published material, new technology outcome needing intellectual property protection, has export control implications, and/or is a country-of-concern technology focus.

Common Indicators and Warnings
- Critical and emerging technology
- New findings yet to be published

Resource Tools
- Travel request form
- Technology match to ODNI-identified country-of-concern technology focus
- Technology match to ASPI-identified country-of-concern technology focus
- Export control of technology for specific organizations

Name of Event and Event Website Information
Requests for attendance at an established conference should include the name of the event, purpose, organizational structure and membership, location, travel information, and nominal conference information for presenters. Other events may be invitational and may not be web enabled. Most conferences are public and international. Events that are bilateral with an organization from or affiliated with a country of concern pose an increased risk.

Common Indicators and Warnings
- Website does not exist or contains scant information for an upcoming conference event
- Event is in or sponsored by a country of concern
- Organization membership contains country of concern organizations
- Organization membership contains malign foreign talent recruitment programs
- Private/invitation-only event with a country of concern organization

Resource Tools

- Website
- Internet search engine
- Know your audience

Event host organization(s)

The host organization should be clearly identified. Those from countries of concern should be reviewed with respect to technology gaps and interests of the host organization. Additionally, the host organization should be reviewed for any affiliations to a malign foreign talent recruitment program.

Common Indicators and Warnings

- Host is from a country of concern
- Host is part of a malign foreign talent recruitment program
- Private/invitation-only event with a country of concern organization

Resource Tools

- Internet search engine
- Risk level through ASPI
- Export control through ITA CSL

Benefits to a home organization

The benefits to a home organization must outweigh the risks. In this case, it is the benefit to the mission and the home organization researcher. This benefit is weighed against the risk of foreign access to the programmatic research and intellectual property.

Common Indicators and Warnings

- AIK from a country of concern
- Not programmatically aligned with scientific mission

Resource Tools

- Travel request form

Foreign Funding Support / Assistance in Kind

In addition to direct monetary payments to the organization for services, indirect monetary support may take different forms including transportation, food, lodging, waiver of any fees (e.g., event registration), or other travel-related expenses.

Common Indicators and Warnings

- Support from a country of concern
- Event in a country of concern

Resource Tools

- Travel request form
- Event website (if available)

Military-Civil Fusion

Military-Civil Fusion (MCF) is a national strategy through which select competitor nations pursue the collection of critical and emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitor nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by acquiring and diverting the world's cutting-edge technologies – including through theft – to achieve military dominance.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies resident within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

Common Indications and Warnings of Foreign Collection Interest

- National strategies (MCF, etc.) targeting emerging technologies (e.g., AI, quantum, bio-economics, autonomous systems, semiconductors, etc.)
- Technology/knowledge gap of competitor nations (e.g., years ahead/behind)
- Competitor nation researchers seeking to collaborate on targeted or knowledge-gap research
- Current or past affiliation of foreign researchers to competitor nation sponsored academic or research institutions and/or foreign talent recruitment programs.

Resource Tools

- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Sponsoring Principal Investigator as the technology subject matter expert
- Senior technical advisors for implications of potential international collaboration (risk/benefit analysis)
- Malign Foreign Talent Recruitment Programs

For virtual travel, a concur decision is forwarded to the requestor with an Overseas Teleconference – Virtual Foreign Travel Checklist (Appendix D). Additionally, where applicable, a suitably secured laptop must be used to attend an event.

7.2.2. Review Process

Figure 4 provides a high-level overview of the research security review process for foreign travel requests, including the risk determination and recommendations (described in more detail in the subsequent Section 8).

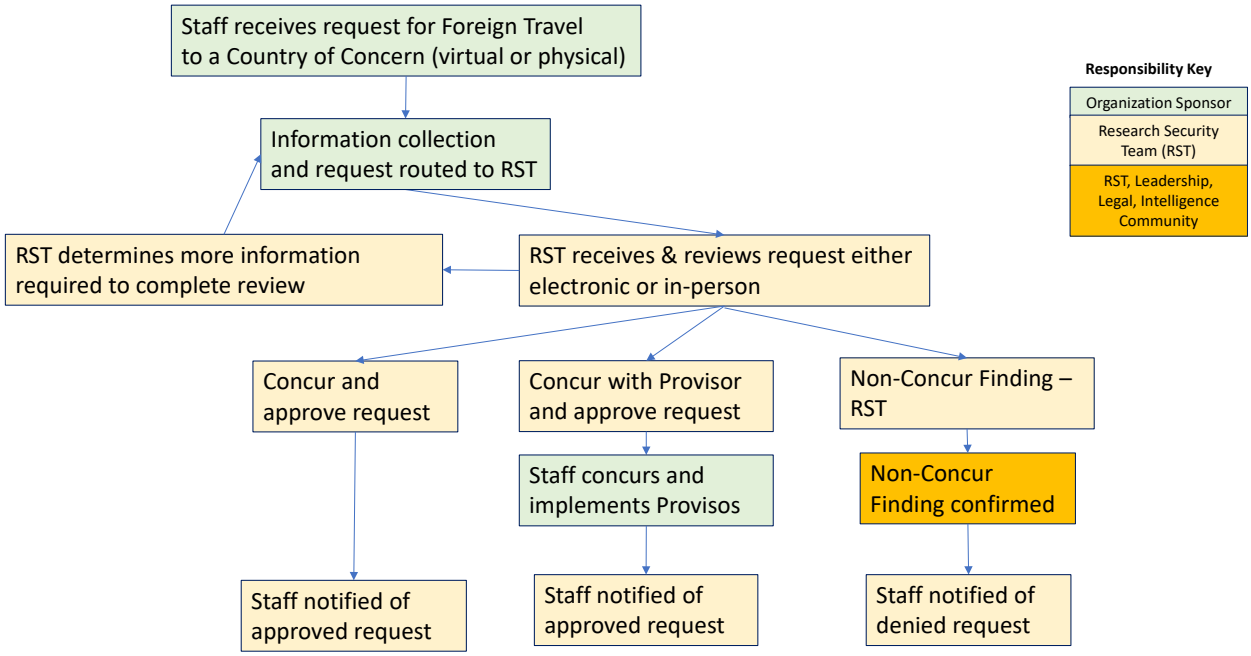

Figure 4. Research security review process for foreign travel.

7.3. Review Category 3: Foreign Collaborations

These reviews are designed to identify the benefit and risk associated with a collaboration engagement with a foreign scientist and their home organization. In most cases, a collaboration will lead to a publication. The collaboration may be bilateral or multinational. In the case of bilateral, the risk of intellectual property theft may occur if the foreign scientist/organization is targeting a military-civil technology gap, where a researcher (e.g., home institution) may be unknowingly asked to perform joint research to solve their missing piece. In the case of a multinational collaboration, there is significantly less risk, and the collaboration is often tied to solving a global scientific challenge and/or concern.

There are two parts to this review, at the beginning of a collaboration and when outcomes are ready for public dissemination (e.g., publications are ready for submission to a technical journal).

7.3.1. Key Questions

Key questions are used to determine whether the benefit of the collaboration outweighs the potential risk. A review reference guide for the key questions is found in the Foreign Collaborations Checklist (Appendix D).

The key question topics are listed below, followed by more detailed descriptions:

- Collaboration participants
- Technology type
- Benefit statement
- Export Control / Technology Control Plan
- Military-Civil Fusion applications
- Patentable outcomes
- Congressional requirements and restrictions
- Research funding source
- Publication

Collaboration participants
Collaborators and their organizational affiliation must be clearly identified. Those from countries of concern should be reviewed with respect to technology gaps and interests. Additionally, an assessment should be conducted on any affiliations between the requesting organization and malign foreign talent recruitment programs. The risk associated with an organization is dynamic and must be checked annually.

Common Indicators and Warnings

- Collaborator is a citizen of a country of concern
- Collaborator is from a high-risk military-civil organization
- Collaborator is part of a malign foreign talent recruitment program
- Bilateral collaboration request from a researcher/organization of a country of concern

Resource Tools

- Internet search engine
- Risk level through ASPI
- Export control through ITA CSL

Technology Type
A determination should be made on whether the research is tied to the Critical Emerging Technology List and the scientific mission of the home organization (see Critical Emerging Technology List and the ODNI Safeguarding Science Toolkit).

Common Indicators and Warnings

- Technology match to ODNI-identified country-of-concern technology focus
- Technology match to ASPI identified country-of-concern technology focus

- Export control of technology for specific organizations

Benefit Statement
The organization needs to determine whether the benefits of the collaboration outweigh the risks. In this case, it is the benefit to the organization, its mission, its nation and its employees. This benefit is weighed against the risk of foreign access to the programmatic research and intellectual property. An agreement that all fundamental research outcomes will be published in the public domain must be established.

Common Indicators and Warnings
- Research outcomes are not expected to be published
- Product and/or service engagement
- Military-Civil application outcomes

Resource Tools
- Home organization subject matter experts
- Home organization technical/scientific leadership

Export Control / Technology Control Plan
Whether classified or unclassified, agencies possess information and technology that requires protection and/or review prior to its transfer. Such information includes export-controlled, proprietary, and other sensitive unclassified information that may be valuable and/or of interest to foreign governments or companies. The Technology Control Plan (TCP) must be approved by the designated export official to ensure compliance with U.S. law and regulatory requirements (EAR/ITAR). For a company, determine whether there are any export control issues (e.g., ITA Consolidated Screening List)

Common Indicators and Warnings
- Scope of research
- Items, software, technology, etc. to be shared
- Research type
- Proprietary or public domain
- Foreign commercial availability

Resource Tools
- International Trade Administration Consolidated Screening List (ITA CSL)
- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Internet Search Engine

Military-Civil Fusion
Military-Civil Fusion (MCF) is a national strategy through which select competitor nations pursue the collection of critical and emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitors

nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by diverting leading-edge technologies through multiple venues such as cyber theft as well as open publications and international collaborative research to accelerate the capability of their commercial and military/defense industries within the global economic environment.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies resident within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

Common Indications and Warnings of Foreign Collection Interest

- National strategies (MCF, etc.) targeting emerging technologies (e.g., AI, quantum, bio-economics, autonomous systems, semiconductors, etc.)
- Technology/knowledge gap of competitor nations (e.g., years ahead/behind)
- Competitor nation researchers seeking to collaborate on targeted or knowledge-gap research
- Current or past affiliation of foreign researchers to competitor nation sponsored academic or research as foreign talent recruitment programs.

Resource Tools

- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Sponsoring Principal Investigator as the technology subject matter expert
- Senior technical advisors for implications of potential international collaboration (risk/benefit analysis)
- Malign Foreign Talent Recruitment Programs

Patentable Outcomes

This question is often used as a tangential question for Military-Civil Fusion applications as the query is directed to the possible commercial use of the technology in question. The researcher is likely more apt to consider patentable applications as a routine aspect of technical progress or maturation. If the PI identifies a possible patentable or commercial application near or at the conclusion of the research project, then there is reason to infer that a Military-Civil Fusion application may also exist.

Congressional Requirements and Restrictions

Examples to consider are based on congressionally funded programs (e.g., CHIPS & Science Act) where research security requirements and restrictions are specifically identified.

Research Funding Source

The funding for the research and for the staff must be determined. Funding for the researchers

and research project may or may not be from the same source. Typical funding sources may include the organization, other USG organizations (e.g., DARPA), universities, industry, and foreign scholarship. For funding from other U.S. organizations (e.g., USG organization or commercial), it is paramount that the funding organization is informed and grants permission for the associate to work on the project. Understanding the funding the proposed collaborator brings to the project is also essential. Certain foreign scholarships are malign and must be avoided; the most common one from a country of concern is the Chinese Scholarship Council.

Common Indicators and Warnings

- Foreign scholarship from a country of concern
- External U.S. funding (e.g., DARPA) focused research
- Funding from a malign foreign talent recruitment program

Resource Tools

- CV/resume of collaborator
- Internet Search Engine
- Persistent Digital Identifiers

Pre-Publication Review

At the end of a collaborative engagement, the publication of the research outcome is reviewed when the authors are from countries of concern. In some cases, the original collaborators reviewed at the beginning of the engagement may not be same at the time of publication. Obtaining a copy of the paper prior to publication may be used to determine if the research outcomes are a critical and emerging technology or a new technology outcome, both of which may need intellectual property protection, may trigger export control considerations, and may be relevant to the country of concern technology focus. For a country-of-concern author, the risk level of the author's organization at the time of publication and whether the author is affiliated with a malign foreign talent recruitment program are considered. Any change to the research funding should be examined as well. A publication may be disallowed if there are clear country-of-concern author ties to a malign foreign talent recruitment program; where the information in the paper is export controlled or enables a country-of-concern MCF technology.

Common Indicators and Warnings

- Country-of-concern authorship and affiliation risk
- Country-of-concern authors not part of research collaboration
- Critical and emerging technology
- Export Control
- Funding from a malign foreign talent recruitment program

Resource Tools

- Home organization subject matter experts
- Home organization technical/scientific leadership
- Technology match to ODNI-identified country-of-concern technology focus
- Technology match to ASPI-identified country-of-concern technology focus

- Export control of technology for specific organizations

7.3.2. Review Process

Figure 5 provides a high-level overview of the research security review process for prepublication review of research papers and related products acknowledging foreign collaboration (described in more detail in the subsequent Section 8).

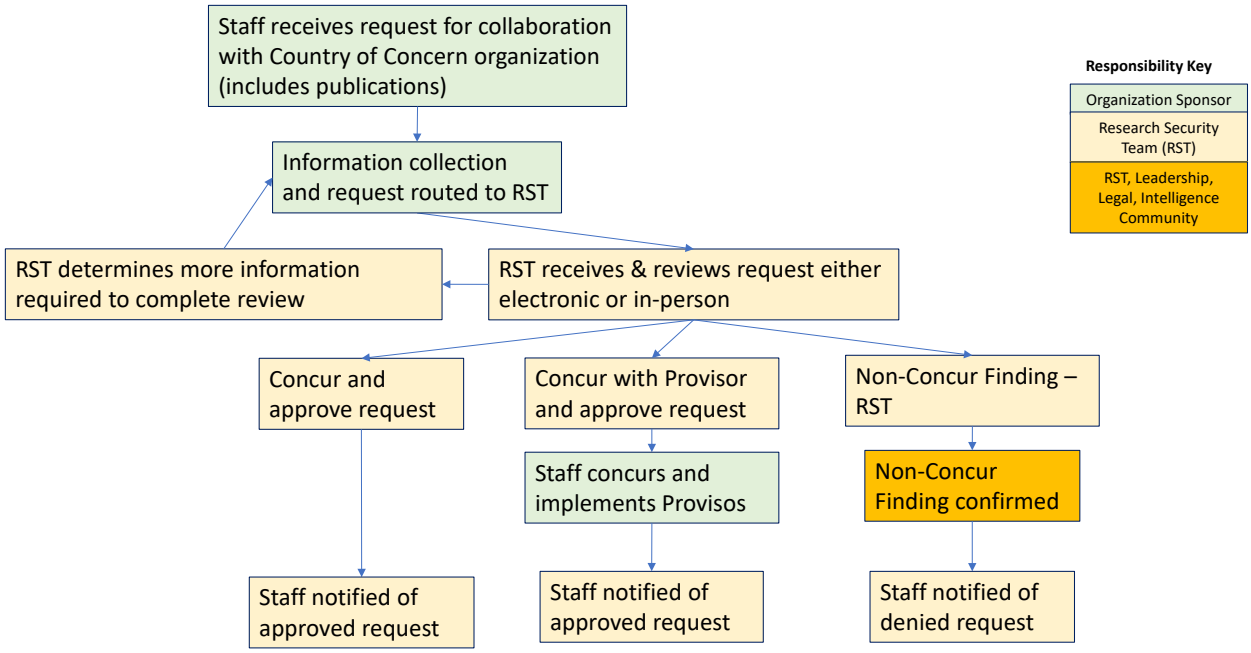

Figure 5. Research security review process for foreign collaborations.

7.4. Review Category 4: Foreign Requests for Products and Services

These reviews are designed to evaluate the benefit and risk associated with an organization's products and services that are internationally disseminated. These may include products produced and sold, services provided, databases, and online research tools. Product and service requests from a country-of-concern organization should be reviewed to recognize any potential MCF technology application or advancement that may occur because of access to that product or service. Additionally, all product and service requests from a foreign organization must be checked for export control license restrictions.

7.4.1. Key Questions

Answers to key questions are used during a review to determine whether the benefit of providing a product or service outweighs the potential risk. The organization's subject matter

expert(s) (SME) and/or technical leadership should provide the responses in the Products, Services, and Software Tools Review Form (Appendix C). A review reference guide for the key questions is found in the Foreign Request for Products, Services, and Software Tools Checklist (Appendix D).

The key question topics are listed below, followed by more detailed descriptions:

- Product/Service
- Requesting Foreign Organization
- Military-Civil Fusion applications
- Export Control

Product/Service
Identify the product or service being requested by a country of concern. The SME should provide information on potential uses of the products or service for military-civil technology applications.

Common Indicators and Warnings

- Military-Civil Fusion application that may create a national or economic security risk
- Requests for source code
- Requests for the same/related product and/or service from multiple country-of-concern organizations
- Requests for large quantities of a product or service

Resource Tools

- Technical SME
- Leadership
- ITA CSL

Requesting Foreign Organization
Requests from countries of concern should be reviewed with respect to technology gaps and interests of the requesting organization. Determine the mission and objectives of the requesting organization and whether the requesting organization has affiliations with a malign foreign talent recruitment program. This may be challenging to ascertain if the country-of-concern organization is using a U.S. subsidiary and/or address. The risk associated with an organization is dynamic and must be revisited for each request.

Common Indicators and Warnings

- Seven Sons of National Defense affiliation and activity level
- ASPI High Risk or Very-High Risk identification
- Malign Foreign Talent Recruitment Program
- Export control

Resource Tools

- Technical SME

- Risk level through ASPI
- Internet search engine

Military-Civil Fusion
Military-Civil Fusion (MCF) [11] is a national strategy through which select competitor nations pursue the collection of critical and emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitor nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by diverting leading-edge technologies through multiple venues such as cyber theft as well as open publications and international collaborative research to accelerate the capability of their commercial and military/defense industries within the global economic environment.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies resident within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

Common Indications and Warnings of Foreign Collection Interest

- National strategies (MCF, etc.) targeting emerging technologies (e.g., AI, quantum, bio- economics, autonomous systems, semiconductors, etc.)
- Dual-use critical emerging technology
- Competitor nation researchers seeking to collaborate on targeted or knowledge-gap research
- Current or past affiliation of foreign researchers to competitor nation sponsored academic or research institutions as foreign talent recruitment programs.

Resource Tools

- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Sponsoring Principal Investigator as the technology subject matter expert
- Senior technical advisors for implications of potential international collaboration (risk/benefit analysis)
- Malign Foreign Talent Recruitment Programs

Export Control
Certain products may require protection and/or review prior to delivery to ensure compliance with U.S. law and regulatory requirements (e.g., EAR/ITAR).

Common Indicators and Warnings

- Devices and/or software requested by a country-of-concern organization

Resource Tools

- International Trade Administration Consolidated Screening List (ITA CSL)
- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Internet Search Engines

7.4.2. Review Process

Figure 6 provides a high-level overview of the research security review process for foreign requests for products or services, including the risk determination and recommendations (described in more detail in the subsequent Section 8).

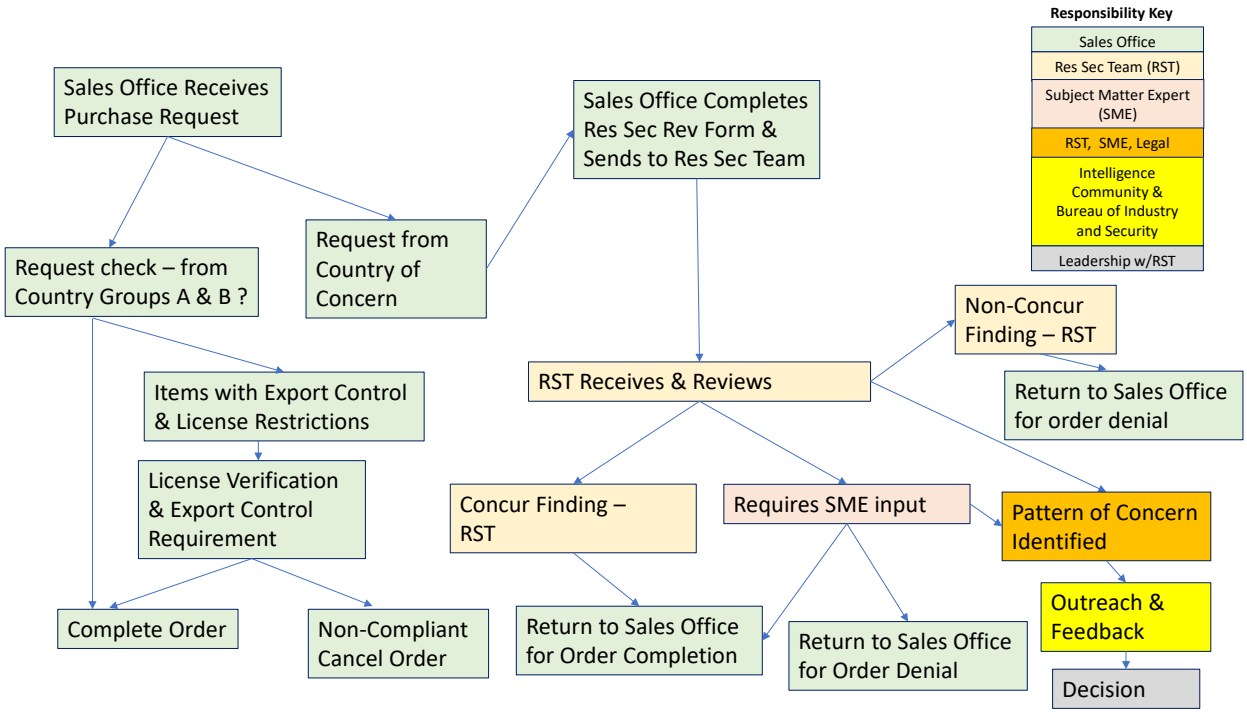

Figure 6. Research security review process for foreign requests for products or services.

7.5. Review Category 5: Extramural Funding Opportunities

An organization may have several types of funding opportunities that are important to mission achievement and that are under the purview of the research security review process. A non-inclusive list of extramural funding opportunities includes contracts, grants, incentives, challenges, and cooperative research and development agreements. The overall funding review methodology described below is designed to be adaptable to any funding type, but specific USG

requirements and restrictions concerning research security applications are briefly summarized (e.g., NSPM-33, CHIPS and Science ACT of 2022).

In accordance with NSPM-33, applicants to USG funding opportunities must adhere to certain research security guidelines.

NSPM-33
The application of NSPM-33 to grants from a Federal Agency (e.g., NSF) is for organizations that receive more than $50M in federal funds [1] [2]. The focus of NSPM-33 is on defining and determining any conflicts of interest and/or conflicts of commitment of a PI applying for a federal grant primarily from academia. The requirements are met through the submission of a list of current and pending support (i.e., all funding related to their research) and a BioSketch (i.e., CV/resume).

For CHIPS and Science Act of 2022 funding incentives, other requirements and restrictions apply to a review process.

CHIPS and Science Act of 2022 (Division A)
The CHIPS and Science Act of 2022 contains specific requirements and restrictions concerning incentives with a foreign organization or person. In general, no organization from or affiliated with a country of concern may apply for an incentive. The CHIPS and Science Act specifically identifies countries of concern as China, Russia, Iran, and North Korea; however, the list of countries of concern and U.S. Department of State Sponsor of Terrorism list is not a constant and should be checked regularly. At the time of this publication, for example, the other country of concern is Belarus and other U.S. Department of State Sponsors of Terrorism are Syria and Cuba.

CHIPS and Science Act Research Security (SEC. 10114)
A paraphrased overview of the salient components of the specific research security requirements listed in the CHIPS and Science Act is provided below. These components must be embedded into an overall safeguarding international science research security program for those participating (e.g., metrology research and development, proposed National Semiconductor Technology Center). While this is under the Department of Energy section, it is useful to apply across the CHIPS and Science ecosystem and does not differ from the Framework in application.

Develop a research security program
- Tools and processes to manage and mitigate research security risks
- Determinations of the risk of loss of U.S. intellectual property or threat to the national security of the United States

Implement research security program
- Deploy risk-balanced approaches to evaluating, awarding, and managing certain research, development, demonstration, and deployment activities

- Designate a person to be responsible for tracking and notifying funding recipients of unmanageable threats to United States national security or of theft or loss of United States intellectual property posed by an entity of concern
- Develop research security training for funding recipients on the risks posed by entities of concern

Department of Commerce Guardrails
The Department of Commerce outlines national security guardrails for the CHIPS and Science Act for America Incentives Program (proposed March 2023).

- The statute prohibits recipients of CHIPS incentives funds from using the funds in other countries
- The statute significantly restricts recipients of CHIPS incentives funds from investing in most semiconductor manufacturing in countries of concern for 10 years after the date of award
- The statute limits recipients of CHIPS incentives funds from engaging in joint research or technology licensing efforts with an organization from or affiliated with a country of concern that relates to a technology or product that raises national security concerns

On 30 September 2022, the SBIR and STTR Extension Act of 2022 – Public Law 117–183 was enacted [12]. Implementation of the SBIR due diligence disclosure requirement includes a form designated as Required Disclosures of Foreign Affiliations or Relationships to Foreign Countries. Completion of this form by an SBIR applicant is part of the information collection process necessary to perform a safeguarding science research security risk-balanced analysis.

The SBIR Due Diligence disclosure requirements are focused on disclosing foreign country engagement necessary to assess security risk. In general, the following is list of information collected.

- Current or pending business arrangements with a foreign country
- Foreign talent recruitment program participation with a country of concern
- Foreign affiliation with any country of concern
- Foreign ownership by country of concern
- Venture capital and/or institutional investment from a country of concern
- Technology licensing or property sales to a country of concern

In general, the review for any funding opportunity is broken down into the main set of key questions and then the ones specific to the intent (e.g., CHIPS and Science Act of 2022, SBIR and STTR Extension Act of 2022, NSPM-33). The review methodology described is applicable to any funding opportunity while meeting the specific USG requirements and restrictions outlined above.

7.5.1. Key Questions

Answers to key questions are used during a review to determine whether the benefit outweighs the potential risk and whether any USG restrictions apply. The answers are supplied by the funding requestor via the Funding Opportunities Review Form (Appendix D) prior to a review. Note that there is an intentional similarity to the foreign associate review process but with the addition of an organizational focus on financial aspects. A review reference guide for the key questions is found in the Extramural Funding Opportunities Checklist (Appendix D).

The key-question topics are listed below, followed by more detailed descriptions:

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

Organization
The name and address of the organization requesting funding.

Requestor
The requestor is nominally the PI associated with the funding request. Information required for review includes:

- Requestor name and position within the requesting organization.
- Current and pending support
- Assistance-in-kind support
- CV/resume
- Foreign Affiliations
- Persistent Digital Identifiers

The current and pending support information is necessary to determine potential conflict of interest and/or conflicts of concern. These conflicts may be within the U.S., foreign, or both. Those potential conflicts with monetary support from a country-of-concern organization will require an increased scrutiny and a determination of intellectual property risk.

Determining the existence of foreign affiliations is necessary to understand the potential for conflicts of interest or commitment. Affiliations include any past or present organization (foreign and domestic) with whom the applicant has a formal relationship or obligation (e.g., universities, scholarships, professional societies, foreign talent recruitment programs).

The risk associated with competitor nation-sponsored university or professional-organization affiliation is dynamic and must be revisited annually. Risk-based adjudication is factored in multiple ways via the following method:

- Determine the risk level of the affiliated organization
    - Open source reference tools such as the Australian Strategic Policy Institute (ASPI), the ITA Consolidated Screening List , Google Scholar, and a persistent digital identifier (e.g., ORCID) are readily available and can be used to determine whether the applicant is actively publishing through a competitor nation sponsored university and/or if any foreign funding (e.g., scholarships, grants) exists
- Determine whether a foreign talent recruitment program is malign. Affiliation with a malign foreign talent recruitment or placement program is considered high risk, and the risk will likely outweigh the benefit of the applicant's participation
- Determine whether there are any export control concerns (e.g., ITA Consolidated Screening List)

Common Indicators and Warnings

- Past or on-going affiliations with competitor nation sponsored entity or organizations
- Funding (e.g., scholarships or grants) from competitor-nation-sponsored entity or organizations
- Contractual agreements with competitor-nation-sponsored entities or organizations (e.g. malign foreign talent recruitment or placement program).
- Inclusion on USG Export Control consolidated screening or entity list

Resource Tools

- CV/resume
- ASPI/Google Scholar/Persistent Digital Identifiers
- Social media
- ITA CSL

Technology Type

It is essential to determine whether any correlation exists between an applicant's foreign affiliations and targeted emerging USG technologies (See Critical Emerging Technology List and the ODNI Safeguarding Science Toolkit).

Common Indicators and Warnings

- Match between applicants' technology of interest and competitor-nation targeted technology
- Applicant's inclusion on ITA CSL

Project Plan
The project plan is a short explanation of the work. It is an overview of the research and specifies the character of the research as either fundamental or applied.

Common Indicator and Warning

- Country of concern interest in identified technology

Export Control / Technology Control Plan
Whether classified or unclassified, agencies possess information and technology that requires protection and/or review prior to its transfer. Such information includes export-controlled, proprietary, and other sensitive unclassified information that may be valuable and/or of interest to foreign governments or companies. The applicant must be compliant with U.S. law and regulatory requirements (e.g., EAR/ITAR).

Common Indicators and Warnings

- Scope of research
- Items, software, technology, etc. to be shared
- Research type
- Proprietary or public domain
- Foreign commercial availability

Resource Tools

- International Trade Administration Consolidated Screening List (ITA CSL)
- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Internet Search Engine

Military-Civil Fusion
Military-Civil Fusion (MCF) is a national strategy through which select competitor nations pursue the collection of critical and emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitor nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by diverting leading-edge technologies through multiple venues such as cyber theft as well as open publications and international collaborative research to accelerate the capabilities of their commercial and military/defense industries within the global economic environment.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies resident within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

Common Indications and Warnings of Foreign Collection Interest

- National strategies (MCF, etc.) targeting emerging technologies (e.g., AI, quantum, bio- economics, autonomous systems, semiconductors, etc.)
- Dual-use critical emerging technology
- Competitor-nation researchers seeking to collaborate on targeted or knowledge gap research
- Current or past affiliation of foreign researchers to competitor nation-sponsored-academic or research institutions as foreign talent recruitment programs.

Resource Tools

- Annual Threat Assessment of the U.S. Intelligence Community
- Australian Strategic Policy Institute (ASPI) Chinese Defense University Tracker
- Malign Foreign Talent Recruitment Programs

Patentable Outcomes

This question is often used as a tangential question for Military-Civil Fusion applications as the query is directed to the possible commercial use of the technology in question. The researcher is likely more apt to consider patentable applications as a routine aspect of technical progress or maturation. If the PI can identify a possible patentable or commercial application near or at the conclusion of the funded opportunity, then there is reason to infer that a MCF application may also exist.

IT Security and Cybersecurity

An organization's research security program must integrate information technology (IT) security system elements, including cybersecurity. Implementing both cybersecurity and IT security best practices creates a risk-balanced approach to determine logical access to science and research information resources, as well as how and when that access is managed.

Examples of IT non-intrusive countermeasures include:

- Limit the use of personally owned devices on the host organization's network to internet use only with no connection to internal organization systems
- Monitor remote access to an organization's network [e.g., User Activity Monitoring (UAM)]
- Recognize the sensitivity of data and restrict proprietary information to authorized networks and personnel only
- Meet IT-applicable export control requirements (EAR)

Common Indicators and Warnings

- Attempted unauthorized access to contiguous research projects
- Requests to access research project space not related to their research
- Requests for elevated privileges

Resource Tools

- NIST Cybersecurity suite of standards, guidelines, and resources
    - IT Access Control System
    - Network Connectivity and Access Monitoring

- User Activity Monitoring

Financial

This applies to an organization's financial business. Understanding whether any direct or indirect foreign ties with a country of concern is part of the risk assessment that may be subject to specific USG requirements and restrictions. Collecting financial information is critical to understanding foreign interference or influence. For example, a country of concern may target a specific intellectual property to fill a MCF technology knowledge gap either through obtaining ownership or business contractual requirements. The following is a list of information that must be part of the submitted funding request and review process for any USG funding opportunity to an organization. Third-party resource tools may be used to validate financial ties and disclosed information contained in the submitted funding request.

- *Ownership*
  Clearly indicate primary organization name, location, and contact information.

- *Subsidiaries*
  Requesting subsidiary organization(s) should identify the primary organization. Additionally, the primary organization should provide a list of subsidiary organizations.

- *Partnerships and affiliations*
  Disclose any organizational partnerships or affiliations with a country of concern.

- *Obligations*
  Disclose any organizational contractual requirements or loans with a country of concern.

Common Indicators and Warnings

- Financial ties to a country-of-concern organization
- Undisclosed financial ties to a country-of-concern organization

Resource Tools

- Current and pending support disclosure form
- Internet search engines
- Third-party financial analytics platform

Long-term maintenance

An internal review for awarded funding opportunities is mandatory. One year is the suggested interval, but substantive changes to answers to key questions for the funded opportunity answers to key questions should trigger a review. *The review is to be treated as new each time to prevent complacency over time.*

7.5.2. Review Process

Figure 7 provides a high-level overview of the research security review process for extramural funding opportunities, including the risk determination and recommendations (described in more detail in the subsequent Section 8).

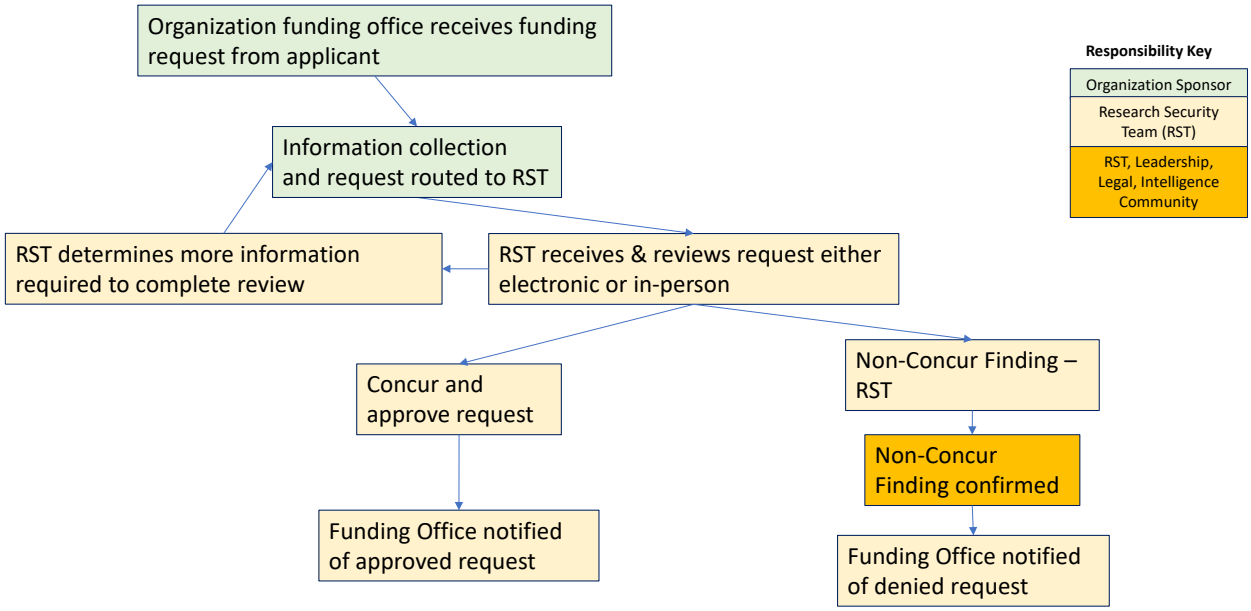

Figure 7. Research security review process for extramural funding opportunities.

8. Risk-Balanced Determination

An amalgamation of information collected during the review process creates the ability to perform a composite-analysis research security review that does not rely on one or two tools and is effective against false-risk positive/negative. A false risk positive/negative occurs when there is a reliance on one "favorite" tool that cannot provide answers to all the key questions. Reliance across multiple tools and sources to garner meaningful answers to the key questions creates data with low uncertainty while emphasizing the "Why" of a determination. The composite analysis is greatly enhanced by including internal staff (e.g., sponsor, subject matter experts, and management) to provide feedback during a review. The collected information from OSINT sources, internal [SMEs and external (e.g., IC)], enables a research security team to understand and balance the benefits to the organization against the potential risks (e.g., active foreign affiliation, military-civil application, etc.) to reach a risk-balanced determination and implement countermeasures.

8.1. Understanding the Risk

Across the science continuum from basic to applied research, to technology solutions, to manufacturing, to documentary/product standards development, there are intersection points of USG agencies, academia, and industry. A vertically integrated research effort may include one to three of the following components:

- Fundamental – theory and experimental combine to create next-generation science
- Applied R&D – translating fundamental concepts to industry applications
- Metrology & Standards – drives 85% of the global economy

All three are inherently connected and dependent upon engagements with industry partners, academic collaborators (both foreign and domestic), and international institutes (e.g., National Metrology Institutes). At the same time, these engagements create vulnerabilities to theft of intellectual property. Addressing research security needs requires knowledge of critical and emerging technologies within the applicable science space:

- What they are?
- Which ones are important?
- Where will they be in five years?
- What technology or knowledge gaps exist that competitor nations need for their Military-Civil-Fusion applications?

The risks to U.S. technical leadership and research integrity materialize in three principal concentrations: national security, economic security, and the safeguarding of intellectual property. It is essential that staff understand all three concentrations and how the mission of the organization as well as the specific research programs and projects integrate and drive critical and emerging technologies. These risks must be considered when evaluating engagement activities, in particular any military-civil applications and patentable outcomes.

National Security
Loss of intellectual property that fills a knowledge gap in a foreign military technology need will create a loss of U.S. technical advantage. This includes the transfer of fundamental research compiles to accelerate foreign military applications.

Economic Security
Unauthorized diversions that weaken the U.S. innovation base and threaten economic competitiveness and threaten U.S. leadership in emerging science and technology. This includes the transfer of fundamental research compiled to accelerate foreign civil applications.

Intellectual Property Security
Some foreign governments violate core principles of integrity and pose risks to the U.S. research enterprise. The use of non-traditional collection methods includes malign foreign talent recruitment, or "Brain Gain" programs, which facilitate the transfer of original ideas and intellectual property from U.S. industry, universities, and research centers. Competitor nations will continue to pursue foreign science and technology information and expertise, making extensive use of foreign scientific collaborations and partnerships, investments and acquisitions, economic espionage, and cyber theft to acquire and transfer intellectual property and technology.

The nominal risk components for consideration under the Framework are listed in Table 5 and described below.

Table 5. Nominal risk components that may negatively impact national security, economic security, or intellectual property security.

Non-Traditional Information Collectors (NTICs)
Critical and Emerging Technologies (CETs)
Technology Gaps
Conflicts of Interest
Conflicts of Commitment
Cybersecurity Risk
Physical Access
Insider Threat
External Organizations
External Funding
Patterns of Concern
Intellectual Property
NIST Cybersecurity Program Suite
NSPM-28 Operations Security (OPSEC) Program
User Activity Monitoring (UAM)

Non-Traditional Information Collectors (NTICs)
NTICS are individuals whose primary profession is not intelligence collection but who collect sensitive U.S. technologies and information on behalf of foreign adversaries – in particular, critical and emerging technologies. Often these are non-career intelligence professionals who seeks to collect U.S. technical data and intellectual property on behalf of competitor nations or other foreign entities through several different collection methods: foreign student/scientist exchange programs, cyber & social media deception, professional conferences, malign foreign talent recruitment (brain gain) programs, and malign foreign talent placement programs. The NTICs are often motivated by their national ideology or strategy and monetary support (e.g., grants, awards, scholarships). Potential foreign national associates are reviewed for backgrounds that could imply a desire to collect such information from the host organization to inform a country of concern.

> Means and methods: NTICs may self-sponsor or be financed through a grant, fellowship, or scholarship.
>
> Indicators and warnings: NTICs typically establish and maintain affiliations with suspected technology collection organizations (e.g., defense-aligned foreign university), go on frequent or unexplained foreign travel, pursue invitations to overseas technical conferences or events, attempt to enable visitors from countries of concern, seek to collaborate or publish papers concurrently with known or suspected technology collectors, attempt to obtain access to equipment (e.g., especially export controlled) or workspaces beyond their authorized program/project scope or need-to-know, attempt to introduce unauthorized recording devices into workspaces, and attempt unauthorized photocopying or downloading of program/project data.

Critical and Emerging Technologies (CETs)
According to the USG, critical and emerging technologies are a subset of advanced technologies that are potentially significant to U.S. national security. A current list of CETs may be found in a recent National Science and Technology Council report [13]. If a foreign associate or affiliated entity is proposing to work on research related to a CET, then a review concerning a technology match of the CET with that of the research scope is needed. Understanding the military-civil fusion technology applications with respect to CET research efforts is critical to understanding and determining the balance of benefits and risks.

Technology Gaps
Critical and emerging technologies are often solutions to technology gaps that a foreign country needs as part of their military-civil fusion technology program to achieve national military and economic superiority.

Conflicts of Interest
According to the 18 U.S.C.§208, a conflict of interest is a personal interest or relationship that conflicts with the faithful performance of official duty. – Situation in which an individual, or the individual's spouse or dependent children, has a significant financial interest, or financial

relationship that could directly and significantly affect the design, conduct, reporting, or funding of research [2].

Conflicts of Commitment
A conflict of commitment is a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time beyond normal institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment [2].

Cybersecurity Risk
A cybersecurity risk is an effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information (or control) systems and reflect the adverse impacts to organizational operations (e.g., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on ISO Guide 73 [14] and NIST SP 800-60 Vol. 1 Rev. 1 [15])

Physical Access
The access to the organizations physical assets granted to a foreign associate depends upon the sensitivity of the proposed research and resources located within the designated spaces. For example, NIST foreign associates are not generally granted after-hours access to campus or access to laboratory or research spaces outside of their immediate need.

Insider Threat
An insider threat is an individual who is a permanent staff member or a long-standing associate who would normally be considered a ‘trusted individual’ who displays behaviors that are contradictory to the well-being of the organization. These behaviors could include partnering with a nefarious organization or foreign entity wishing to do harm to the organization or to the USG.

External Organizations
External organizations are organizational affiliations of a foreign guest researcher. These may include active and passive affiliations such as universities, foreign talent recruitment programs (e.g., benign and malign), malign foreign talent placement programs, as well as government, social, and/or commercial entities.

External Funding
All potential foreign guest researchers are reviewed for the origins of the funds that are supporting their appointments. If an FNA has volunteered to work unpaid or is fully supported by an unknown outside entity, this could represent an attempt to gain insider knowledge into a potential technology.

Patterns of Concern
An anomaly occurs when the data collected during a review is outside the norm of expectations (e.g., exceeds one standard deviation of historical record norm). In this case, the reason for the anomaly cannot be identified with small uncertainty (e.g., ask why and what is the uncertainty in the answer). The identification of a pattern of concern is steeped in understanding the science and the mission of the home organization as well as understanding critical emerging technologies and dual-use technologies (aka military-civil fusion). When a pattern of concern is identified, then the first question is of national security risk – there is or is no concrete evidence (to date) and whether there is enough potential and uncertainty to ask the Intelligence Community to consider the risk. The second question is of economic security and whether the Bureau of Industry and Security (BIS) should be consulted about potential export control considerations.

Intellectual Property
Intellectual property pertains to any original creation of the human intellect such as an artistic, literary, technical, or scientific creation [16].

NIST Cybersecurity Program Suite: NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public. This suite ranges from specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

NSPM-28 Operations Security (OPSEC) Program: The implementation of this Framework integrates the NSPM-28 OPSEC Program strategy as a fundamental construct of a successful research security program whereby the basic principles of the OPSEC process or cycle are employed to determine critical assets needing protection. Employment of the OPSEC cycle therefore can be seen as a mission-focused starting point to determine what intellectual property and technologies are at risk by foreign adversaries seeking to fill a technology knowledge gap using military-civil collection applications. Emerging science and technologies, classified research, export-controlled technologies, and controlled unclassified information (CUI) are all potential indicators of critical assets. With the expanding global competitive environment and spreading dual-use application of emerging U.S. technologies, employment of NSPM-28 risk management strategies will assist to identify critical assets (e.g., intellectual property and technologies), consider the foreign collection threats directed against the critical assets, identify vulnerabilities, risk of exploitation, and employ risk management principles to apply security countermeasures to mitigate vulnerabilities and the possible loss or compromise of intellectual property. OPSEC or any risk management strategy is recognized as an ongoing process whereby emerging threats and the vulnerabilities and risks to those threats are continuously assessed to reinforce the safeguarding science objectives of any research security program.

User Activity Monitoring (UAM)
Every organization has unique information systems or networks that can be monitored to detect suspicious or abnormal activity. UAM consists of proactive measures introduced within the confines of a U.S. Government information system or network as a security countermeasure to monitor inappropriate or suspicious activity by authorized system users. UAM can identify users who may be abusing their system access or otherwise reveal suspicious activity that may indicate a potential insider threat or vulnerability. Any UAM initiative must be implemented with the full understanding and concurrence of the organization's Chief Information Officer.

8.2. Review Recommendation Determination

For an in-person review, the number of research security team members in attendance must be enough to constitute a quorum. Additionally, the Host/Sponsor and at least their supervisor and organizational leadership must attend to constitute a quorum. The organizational leadership may designate an attendee from their headquarter staff to represent them.

At the conclusion of a review, a team adjudication of all risk factors is conducted and a consensus risk level of low, medium, or high is assigned to the program. Program or project risk level may be mitigated by the team assignment of tailored security provisos (e.g., remedial training, supplementary laboratory/workspace physical and logical access reviews, or intermediate progress report). In the case of a concur with provisos determination, there are several nominal options to consider as a function of the risk level. The sponsor and line management are required to concur and implement the specified provisos.

Routine security provisos that can be employed include:

- Operations Security training for all research team members
- Risk Assessment of laboratory and contiguous research project workspaces
- External funding agency approval of foreign participation
- Employment of enhanced User Activity Monitoring
- Shortened program/project review cycle
- Compartmentalization of lead technology or intellectual property
- Limit the program/project access or need-to-know of the foreign participant

Figure 8: Tiered risk mitigation construct.

Final Risk Determination

Team members and required representatives who are present must cast a vote either electronically or during a review meeting. A by-consensus risk determination is reached by the team with the final determination to concur, concur with provisos, or non-concur with the proposed foreign collaboration being recorded by the team lead. A non-concurrence decision for any review requires consultation with organizational leadership (e.g., Director or designee) before the team lead renders a final risk determination.

9. Research Security Risk Determination Matrix

As part of a rigorous research security review process, a risk-balanced determination must be made (see Section 8). This section is intended to provide a Risk Determination Matrix along with a thorough discussion to assist research security practitioners and inform the broader community. This matrix is designed to assist the research security practitioner in making a risk-balanced determination that is consistent with the Framework and therefore provides an integrated, mission-focused, and risk-balanced approach for safeguarding international science and technology from undue foreign interference while protecting the openness and integrity of the U.S. research ecosystem. The Risk Determination Matrix is meant to serve as a tool to assist the practitioner in reaching independent (and defensible) risk determination(s). In this regard, it facilitates the final risk determination, but its use requires certain conditions be met prior to its implementation. This chapter will provide an explanation of all the components that go into making a risk-balanced determination to support the use of the Risk Determination Matrix. This includes discussions of the following outcomes expected of a Research Security Risk Determination:

- Risks
- Findings
- Guidance
- Clarifications
- Mitigations
- Recommendations

A research security review necessitates a well-informed research security practitioner. First and foremost, an understanding of the current “State-of-the-art" for the science or technology under consideration is essential. This implies a need a for a certain degree of subject matter expertise. Where the research security practitioner may not readily possess the necessary level of subject matter expertise, it is recommended to consult home organization subject matter experts or technical/scientific leadership. Secondly, the Risk Determination Matrix needs to be recognized as a tool that is designed to assist the research security practitioner in reaching an independent, and defensible, risk determination. In this regard, it is not a score-based assessment, rather it is designed to permit latitude in as a practitioner makes recommendation.

9.1. Scope of the Risk Determination Matrix

The Risk Determination Matrix is designed to be flexible to mission centricity and adaptable to the various categories of cases that a research security practitioner may be asked to consider. In this regard it can be applied to the individual components of a research security program or as a comprehensive assessment tool to inform the risk determination of the five different research security review categories mentioned in Section 7. These categories along with their subsections are:

- Research Associate Appointments [7.1] – Covered Individuals
- Foreign Travel Requests [7.2] – virtual and physical
- Foreign Collaborations [7.3] – and publications
- Foreign Requests for Products and Services [7.4]
- Extramural Funding Opportunities [7.5] – Grants, Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Agreements, Other Transactional Agreements, Material Transfer Agreements

9.2. Application of the Risk Determination Matrix

In applying the Risk Determination Matrix, it is necessary to understand its intent. Within the Risk Determination Matrix, no numerical values are assigned to risk factors. Rather, the research security practitioner is challenged to apply their own experience(s) and expertise to arrive at a risk determination based on their best judgement of the criticality of the technology, known foreign collection risk, and open-source intelligence (OSINT) fact-based indicators. In pursuit of this goal, the Risk Determination Matrix acts as an educational tool intended to baseline or otherwise standardize a practitioner's tradecraft. Risk determinations will naturally differ based on factors such as thoroughness and the experience of the research security practitioner, as well as individual knowledge, judgement, and expertise. The Risk Determination Matrix is intended to assist the research security practitioner in reaching a holistic, fact-based, and defensible Research Security Risk Determination.

With respect to a Risk Determination, it is critical to maintain a focus on the science or technology under consideration. It's all about the science. By maintaining this approach along with clearly communicating the importance of research security, and ensuring a transparent process, it becomes possible to build a research security culture. The Risk Determination is one piece of this culture and the communication of the determination, and the review process can help support a culture that safeguards national security and economic security, as well as the intellectual property of a researcher.

National Security
Loss of intellectual property that fills a knowledge gap in a foreign military technology need will create a loss of U.S. technical advantage. This includes the transfer of fundamental research compiled to accelerate foreign military applications.

Economic Security
Unauthorized diversions that weaken the U.S. innovation base and threaten economic competitiveness and threaten U.S. leadership in emerging science and technology. This includes the transfer of fundamental research compiled to accelerate foreign civil applications.

Intellectual Property Security
Some foreign governments violate core principles of integrity and pose risks to the U.S. research enterprise. The use of non-traditional collection methods includes malign foreign talent recruitment, or "Brain Gain" programs, which facilitate the transfer of original ideas and

intellectual property from U.S. industry, universities, and research centers. Competitor nations will continue to pursue foreign science and technology information and expertise, making extensive use of foreign scientific collaborations and partnerships, investments and acquisitions, economic espionage, and cyber theft to acquire and transfer intellectual property and technology.

The Risk Determination Matrix (Table 6) is built upon the factors and risks that are considered during the course of a research security review. The principal categories considered are Technology, Organization, and Individual.

For each of the principal categories, a search of open-source intelligence is used to generate a list of Findings, where a trained research security practitioner recognizes Indicators and Warnings.

The acronym RAFT: Recruitment, Affiliations, Funding, and Technology, can be a useful tool to assist in recognizing potential Indicators and Warnings.

Recruitment

- How were you approached?
- Multinational or bilateral?
- Programmatically aligned with your research or theirs?

Affiliation

- Are their affiliations benign or malign?

Funding

- What is the source of funding – theirs or yours?

Technology

- What are the potential commercial and military/civil fusion applications?
- Does it fill a knowledge gap they need to advance their military/civil objectives?

The Risk Determination Matrix (Table 6) is structured in such a way that the rows correspond to the Technology, Organization, and Individual, while the columns for indicators and warnings (or Research Security Review Findings) are organized in order of increasing risk from left-to-right: Low Risk, Medium risk, and High Risk.

Table 6. Research Security Risk Determination Matrix

	Low Risk Indicators	Medium Risk Indicators	High Risk Indicators
Technology	• No, Limited, or appropriately protected Mil/Civ applications • No export control concerns • Basic research • Technology Readiness Level (TRL) 1 or equivalent	• Longer term military impacts (low TRL: 2 to 4) • Significant patentable/commercial applications relevant to economic security (e.g., Critical and Emerging Technology (CET) with respect to ODNI Annual Threat Assessment) • Export control	• Nearer term military applications (higher TRL: ≥4) • Significant patentable/commercial applications relevant to economic security and national security (e.g., CET with respect to ODNI Annual Threat Assessment) ○ Technology targeted by malign actors
Organization	• No Foreign Entity of concern (FEOC), Foreign Country of Concern (FCOC), or malign foreign involvement	• Past FEOC, FOCI, or malign foreign affiliations • Substantial foreign venture capital/joint ventures • Overseas research facilities • Limited foreign ownership/board members	• Current FEOC, FOCI, or malign foreign affiliations • Substantial potential malign foreign venture capital / joint ventures • Substantial foreign ownership or foreign board members ○ Potential foreign monopsony control
	• **Technology/IP Protections.** Strong research security, export control protections, etc. • Stated compliance with NIST cybersecurity standards	• BIS unverified list • Incomplete/insufficient technology control program plan / scoped to proposed research • Evidence of malign foreign interests having access to research facilities or project data • Documented cybersecurity breaches or physical security violations	• Identified history of export control violations • Evidence of malign foreign interests having access to research facilities or project data • Documented cybersecurity breaches or physical security violations
Individual	• **FEOC / MFTRP.** No evidence of FEOC or Malign Foreign Talent Recruitment Program (MFTRP) involvement	• Past affiliation/signed agreement with an MFTRP	• Failure to disclose information • Evidence of deliberate deception • Current affiliation / signed agreement with an MFTRP
	• **Conflict of Interest/Commitment** No malign foreign affiliations • Associations or affiliations	• Past partnerships, contracts, research, or affiliations with FCOC universities or with FCOC military entities	• Current partnership(s), contract(s), research, or affiliation(s) with FCOC universities or with FCOC military entities • Substantial malign foreign publications / patenting in technology areas of concern
	• **Research Integrity.** Information in Current and Pending Support (C/PS) forms and resumes/CVs validated	• Incomplete information	• Evidence of fraud, misdirection, or misappropriation of funding for research • Failure to disclose after requests for additional information or clarification
Conclusion	**Minimal Mitigations Possible**	**Limited Mitigations Required**	**Significant Mitigations Required**

9.3. Technology

The Research Security Risk Determination begins with the technology, or science, being considered. Here, the Critical and Emerging Technologies List Update from February 2024, can serve as an initial guide, as it is rather comprehensive. Any type of military-civilian (mil/civ) fusion and whether the technology may have dual-use applications or be subject to export control must be considered.

Military-Civil Fusion (MCF), as defined by the U.S. Department of State, is a national strategy through which select competitor nations pursue the collection of critical and emerging technologies through both lawful and illicit means to advance their economic and national security objectives. To advance MCF, competitor nations acquire the intellectual property, critical technologies, and advanced research, not only through their own science and research initiatives, but by acquiring and diverting the world's cutting-edge technologies – including through theft – to achieve military dominance.

A viable research security program must be conscious of the asymmetric foreign collection threats directed against its agency, staff, and intellectual property. PIs should be prepared to define critical and emerging technologies residing within their research projects or programs, including fundamental research that may have dual-use applications within the next five years and that a competitor nation might exploit to accelerate its own economic or national security interests.

In addition to military-related defense applications, potential commercialization opportunities should also be considered as economic security concerns can arise from continued realization of new technologies. Here the Sponsoring Principal Investigator, Program Manager, or other internal technology subject matter expert can be essential in assessing the potential for such applications. An understanding of the current state of the art, as well as any current critical gaps or unsolved challenges, is essential to assessing research security risks associated with any technology. The Critical and Emerging Technologies List Update identifies priority technology subfields and is intended to be updated no less than every two years. Knowledge of the research landscape on the international scale has the added benefit of providing a comparison between the domestic and international capabilities. At another level, it is critical to consider if the technology is an identified target of a Foreign Country of Concern. In cases, where a Foreign Country of Concern is known to be aggressively pursuing a technology, the risk can become greater. Finally, the Technology Readiness Level (TRL), see Figure 9, provides a concept of the maturity of the technology in terms of where it lies from Fundamental Research (TRL 1) to Early Adoption (TRL 9). Given the possibility of nearer term applications, risk can increase when a technology is closer to adoption compared to exploratory research. According to NSDD 189:

> *"Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development,*

design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

However, the designation of Fundamental Research does not imply that such research has inherently zero risk. Fundamental Research can be considered the building blocks that provide the base for key advancements in Science and Technology.

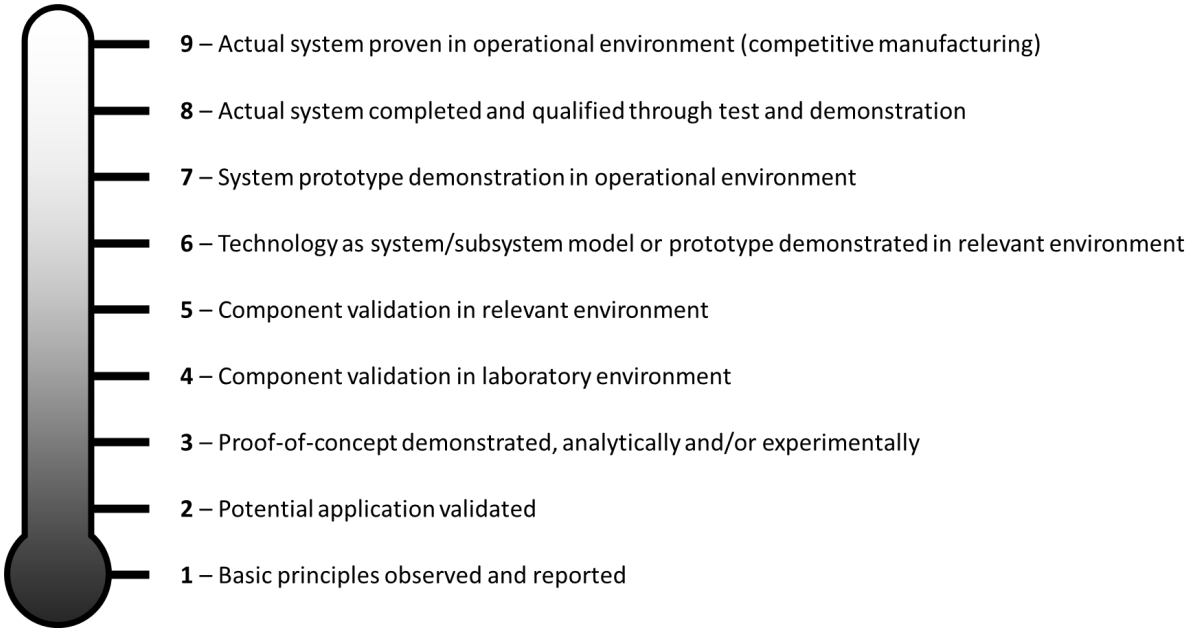

Figure 9. Technology Readiness Levels (TRLs).

Technology Low Risk Indicators

- Basic research
- No, limited, or appropriately protected mil/civ applications
- Technology is not identified to be subject to export control
- TRL 1 or equivalent

Technology Medium Risk Indicators

- Longer term military impacts (low TRL, 2 to 4)
- Significant patentable/commercial applications relevant to economic security (e.g., CET)
- Developing technology may be subject to export control

Technology High Risk Indicators

- Nearer term military applications (higher TRL, > 4)
- Significant patentable/commercial applications relevant to economic security (e.g., CET)

- Technology targeted by malign actors – types include information technology, robotics, aerospace, ocean engineering,
- Technology currently subject to export control

Resource Tools

- Subject Matter Experts (Principal Investigator(s), Program Manager(s), other internal technology subject matter experts)
- Critical Emerging Technology List and the ODNI Safeguarding Science Toolkit
- Senior technical advisors for implications of potential international collaboration (risk/benefit analysis)
- Annual Threat Assessment of the U.S. Intelligence Community
- Export Administration Regulations (EAR)

9.4. Organization

The second category of the Risk Determination Matrix is any involved Organizations. At the Organization level, there are two principal aspects to consider: (1) Foreign Entities of Concern(FEOC) or Foreign, Ownership, Control, or Influence (FOCI); and (2) Technology/IP Protections. The first aspect focuses on potential pathways for foreign interference or influence on an organization. The second aspect focuses on the organization's capacity to protect its technology. Together, these aspects encompass research security risks at the institutional level.

The identification of an entity as a FEOC can be a relatively straightforward process, where maintained lists such as those from the International Trade Administration (ITA), Department of War, or other security-focused organizations can be used as a reference. However, it is critical to consider the possibility of hierarchical organizations, that may include parent and child organizations, subsidiaries, etc. By comparison, the identification of FOCI can be a complicated process due to the various ways that these can manifest. Ownership, and to a lesser extent Control, can be ascertained by considering board members and investments, including mergers and acquisitions. Venture capital investments should be carefully examined for possible connections to Foreign Countries of Concern (FCOCs). Influence can take many forms, such as a foreign monopsony, foreign joint ventures, and overseas research facilities, as well as other subtle methods, which may include the use of shell companies or false front organizations to hide possible Indicators and Warnings.

Organization Low Risk Indicators

- FEOC/FOCI
  - No FOCI – No FEOC, FCOC, or malign foreign involvement

- Technology/IP Protections
  - Strong research security, export control, etc.
  - Stated compliance with NIST cybersecurity standards

Organization Medium Risk Indicators

- FEOC/FOCI
  - Past FEOC, FOCI, or malign foreign affiliations
  - Substantial foreign venture capital/joint ventures
  - Overseas research facilities
  - Limited foreign ownership/board members (sources of influence)

- Technology/IP Protections
  - Identified history of export control violations
  - BIS unverified list
  - Incomplete technology control program plan / scoped to proposed research
  - Insufficient technology protection program
  - Evidence of malign foreign interests having access to research facilities or project data
  - Documented cybersecurity breaches or physical security violations

Organization High Risk Indicators

- FEOC/FOCI
  - Current FEOC, FOCI, or malign foreign affiliations
  - Substantial potential malign foreign venture capital / joint ventures with significant financial influence and programmatic influence
  - Substantial foreign ownership or foreign board members
  - Potential foreign monopsony control

- Technology/IP Protections
  - Identified history of export control violations
  - Evidence of malign foreign interests having access to research facilities or project data
  - Documented cybersecurity breaches or physical security violations

Resource Tools

- Internet search engine
- DOC International Trade Administration Consolidated Screening List
- Australian Strategic Policy Institute "China Defence Universities Tracker"
- Securities and Exchange Commission filings (EDGAR)
- Financial databases
- DoD 1286 List
- DoD 1260H List (List of Chinese military companies)
- Government of Canada's Named Research Organizations List

9.5. Individual

The third and final category of the Risk Determination Matrix is any Covered Individuals. Here an understanding of the Covered Individual's community is essential to properly interpreting any indicators or warnings, where those indicators or warnings can differ drastically depending upon their background and current employment. For example, an academic researcher's status/background can change significantly over the course of their career, while industry researchers and startup founders can exhibit similarly dynamic backgrounds, but Covered Individuals coming from different areas will have unique potential indicators or warnings. The first step is to check if the Covered Individual has been identified as a FEOC or is currently, or was in the past, affiliated with a Malign Foreign Talent Recruitment or Placement Program. Here, disclosure of a past affiliation should be evaluated appropriately. In the interest of promoting transparency between covered individuals and the research security practitioner, active affiliations are considered to be cause for concern, while past affiliations may not be, unless there is a strong pattern. Research Integrity is a key component to a healthy research system, and as so, it is an important consideration within the context of research security reviews.

Within the research community, patents, publications, and presentations can serve as a proxy to consider research collaborations. Given the proximity of patents to nearer term applications, the location of where patents are filed, who they are with, and when they are filed can be an important indicator or warning. Recent co-authorship on publications can be useful tools to begin looking for collaborations or potential Conflicts of Interest or Conflicts of Commitment, but the inherent degree of uncertainty necessitates a critical assessment. The career stage of an individual must be understood along with cultural norms inherent to the scientific community. Also, the publication dates should be carefully considered with recognition for the time it takes to publish compared to when collaborative work may have been performed. Similarly, co-authored Conference Presentations/Proceedings can be considered, but as stated earlier, there must be recognition of the ambiguity and any potential conclusions drawn should be well-supported by other sources. A significant number of Invited Talks/Seminars FCOCs can indicate ongoing and/or enduring professional relationships, and when combined with the exchange of visiting researchers, potential pathways for the transfer of knowledge become more apparent.

Individual Low Risk Indicators

- Foreign Entity of Concern / Malign Foreign Talent Recruitment Program
  - No evidence of FEOC or MFTRP involvement
- Conflict of Interest/Commitment
  - No evidence of Conflicts of Interest or Conflicts of Commitment
  - No malign foreign associations or affiliations
- Research Integrity
  - Information in Common form for Current and Pending (Other) Support Information and Biographical Sketch/resumes/CVs validated

Individual Medium Risk Indicators

- Foreign Entity of Concern / Malign Foreign Talent Recruitment Program
  - Past affiliation/signed agreement with an MFTRP
- Conflict of Interest (Money/Funding)/Commitment (Time)
  - Past partnerships, contracts, research, associations, or affiliations with FCOC universities or with FCOC military entities
  - Continuing historical pattern of substantial malign foreign publications / patenting in technology areas of concern
  - Dual funding US and FCOC for same project
- Research Integrity
  - Incomplete information in provided C/PS forms and resumes/CVs

Individual High-Risk Indicators

- Foreign Entity of Concern / Malign Foreign Talent Recruitment Program
  - Failure to disclose information
  - Evidence of deliberate deception
  - Current affiliation / signed agreement with an MFTRP
- Conflict of Interest/Commitment
  - Current partnership(s), contract(s), research, or affiliation(s) with FCOC universities or with FCOC military entities
  - Current substantial malign foreign publications / patenting in technology areas of concern
- Research Integrity
  - Evidence of fraud, misdirection, or misappropriation of funding for research
  - Failure to disclose after requests for additional information or clarification
  - Refusal to sign the common form

Resource Tools

- Suppled Biographical Sketch/resume/curriculum vitae (CV)
- Current and pending support forms (Common form for Current and Pending (Other) Support Information)
- Publication databases
- Patent databases
- Center for Security and Emerging Technology Chinese Talent Program Tracker
- Professional network platform (e.g., LinkedIn, ResearchGate, etc.)

With respect to individuals, it may again be helpful to remember the acronym RAFT: Recruitment, Affiliations, Funding, and Technology to identify Indicators and Warnings.

Recruitment

- How were you approached?
- Multinational or Bilateral?
- Programmatically aligned with your research or theirs?

Affiliation

- Are their affiliations Benign or Malign?
    - Consider publication history (Foreign Entities of Concern or Foreign Countries of Concern)
    - Location of presentations and publications (Foreign Countries of Concern)

Funding

- What is the source of funding (listed in Acknowledgements sections)?

Technology

- What are the potential military/civil fusion applications?
- Do they focus on Critical and Emerging Technologies?
- Does it fill a knowledge gap they need to advance a CET?

9.6. Regarding the Application of Developing Tools

Currently, there is a large focus on automating parts of the research security review process. While this can facilitate rapid analysis, it is critical that these tools be applied as part of the toolkit of a research security practitioner, rather than as a replacement for the entire process. It is critical that a research security review rely on fact-based data analysis to minimize uncertainty. With respect to elevated risk determinations, the identification of indicators, warnings, and even any assessment(s) performed in an automated fashion must always be evaluated with respect to the original data sources. Disambiguation with limited information is an ever-present challenge. As such, any determination(s) made must be made with careful consideration and examination of the original references and sources, rather than based upon a generated summary.

9.7. Using the Risk Determination Matrix

Proper use of the Risk Determination Matrix relies upon the ability to filter through fact-based findings and identify indicators and warnings. These fact-based indicators and warnings then inform the Risk Determination. This Risk Determination Matrix does not rely on a scoring system where weights and numbers are assigned to the various levels for Risk Indicators, in recognition of the adage that, “When a measure becomes a target, it ceases to be a good measure.” Inevitably, when values and score ranges for levels of risk are introduced, they can become the principal focus, to the detriment of making a defensible, fact-based risk determination. Rather, the Risk Indicators of each principal category (Technology, Organization, Individual) should first be considered independently. Then, a Risk Determination is made based

on a modified holistic approach, where the highest identified Risk Level across the Matrix drives the first risk determination and then following that other factors are considered.

The below tables demonstrate examples of how to use the Risk Determination Matrix. First, the Indicators and Warnings that correspond to each Category are collected. Next, the Risk Levels associated with each of the three principal categories are assessed independently. Once this has been completed, the overall risk is determined, with the highest risk category driving the Risk Determination, as can been in Table 7 and Table 8.

Table 7. Sample risk determination – High

Category	Risk Level
Technology	M
Organization	M
Individual(s)	**H**
Overall	**H**

Table 8. Sample risk determination – Medium

Category	Risk Level
Technology	L
Organization	**M**
Individual(s)	L
Overall	**M**

9.8. Risk Determinations

Ultimately, the research security practitioner, with the assistance of the Risk Determination Matrix, will reach a risk-balanced determination that is consistent with the Framework and therefore provides an integrated, mission-focused, and risk-balanced approach for safeguarding international science and technology from undue foreign interference while protecting the openness and integrity of the U.S. research ecosystem. Regardless of the level of risk determined, the central question is always, “Does the Benefit Outweigh the Risk?”

A research security review is a collaborative decision-making process between the Team and organizational management consisting of a risk/benefit recommendation by the Team to organizational management for a final risk determination. The composite analysis of the information acquired and assessed during a research security review results in a risk-balanced determination of low, medium, or high risk contained within the Research Security Review Form. A no risk determination is impractical as achieving a no risk security posture is unrealistic and can be deceptive of underlying risk to customers, asset owners, and research security practitioners.

A low-risk determination concludes that the risk is acceptable and that the benefits to the organization clearly outweigh the risk. A medium risk determination concludes that an identified risk exists, and that the risk can be mitigated through the deployment of available security countermeasures to achieve an acceptable risk/benefit determination. A high-risk determination concludes that a targeted collection risk exists, and that the deployment of available security countermeasures may be insufficient to achieve an acceptable risk/benefit determination resulting in a rejection of the grant application. Targeted high-risk collection threats may require validation from other informed sources.

In recognition of the fact that a risk determination is one piece of the larger effort to safeguard international science, an elevated identified risk level does not necessarily infer a rejection. With a risk-balanced approach, elevated risk levels can require that the research security practitioner make use of additional tools to protect against identified risks.

Once an initial risk determination has been made, the research security practitioner has several tools at their disposal to either support or assist the determination or provide an opportunity to adjust the risk determination based on additional information or actions. These tools include Findings, Clarifications, Recommendations, and Mitigations.

Findings
Findings are the fact-based Indicators or Warnings that inform the risk determinations for each principal category. Subsequently, Findings drive the first risk determination. Findings must be relevant to the scientific field or technology under consideration. Consideration for the Science and Technology drives the research security review process.

Clarifications
Clarifications are any additional questions or requests for information that arise during the initial risk determination. This can include additional information that may reduce the risk determination, missing information, or information that conflicts with or cannot be validated against Findings. Requests for clarification can be a useful part of establishing an open dialog and transparent process.

Recommendations
Recommendations are not required actions but are non-binding suggested courses of action for an improvement to the research security risk for the entity being reviewed. A Recommendation does not impact the risk determination but rather is intended as a long-term effort to suggest research security-related improvements.

Mitigations
Mitigations (or countermeasures) are actions intended to reduce the severity or the effects of identified research security risks. Within the context of a risk-balanced approach, mitigations are targeted required actions that are made at the individual research security review level on a case-by-case basis. While intended to reduce research security risk, mitigations can only reduce the level of the initial risk determination by one level. The introduction of mitigations cannot negate risk unless the cause for mitigation is completely removed.

Routine mitigations that can be used include:

- Operations Security training for all research team members. Topics include:
  - Export control
  - Research security
  - Foreign travel
  - Cyber/IT security
  - Counterintelligence
- Risk Assessment of laboratory and contiguous research project workspaces
- External funding agency approval of foreign participation
- Employment of enhanced User Activity Monitoring
- Shortened program/project review cycle
- Compartmentalization of specific technology(ies) or intellectual property
- Limiting the program/project access or need-to-know of the foreign participant

9.9. Conclusion

The Risk Determination Matrix is intended to serve as a tool to assist the research security practitioner at arriving at a comprehensive and well-informed recommendation that is a key component of the collaborative decision-making process between the Team and organizational management that results in a final risk determination. As such, it is one part of the Research Security Framework that falls within the larger scope, intending to strike a balance between openness, scientific research security, and international collaboration.

10. Records Management and Dissemination Controls

All documents or products originated by the Team should be reviewed to determine whether specific content warrants safeguarding against unauthorized access or disclosure by designation. (e.g., Controlled Unclassified Information (CUI) consistent with E.O. 13556 and 32 CFR Part 2002).

Team-originated documents and products revealing internal research security review processes, methodology, and final risk determinations should be conspicuously marked consistent with the CUI Registry and Information Categories (e.g., CUI//OPSEC//FEDCON/NOFORN) and forwarded to the Team Lead for review and approval prior to publication. See NIST SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Results of reviews should be archived electronically (preferably in a controlled-access shared-network site) with all review records secured to detect and/or prevent unauthorized access and should only be shared with individuals possessing an appropriate need to know.

11. Export Control and Compliance

Host organizations with a scientific research mission that engage in projects concerned with critical and emerging technologies may be subject to U.S. export controls.

Determination that a host organization possesses information and technology that requires protection and/or review prior to its transfer is required. Such information includes export-controlled, proprietary, and other sensitive unclassified information that may be valuable and/or of interest to foreign governments or companies. A Program must ensure that its most valuable equities, including research data, information, and technology, are well protected from inappropriate transfer to its foreign partners and collaborators, and from theft by foreign powers. To this end, agencies should appoint a resident expert on all matters related to export control and international technology transfer to serve as the principal point-of-contact. This expert must maintain a thorough knowledge of current Export Administration Regulations (EAR) and/or the International Traffic in Arms Regulations (ITAR) provisions and requirements and all relevant requirements applicable to the agency's programs and activities and assist in developing policy and procedures as appropriate. It is critical to put controls in place to ensure that transfer of export-controlled information or technical data under the purview of the EAR or the ITAR does not occur unless authorized by the appropriate regulating agency.

Where applicable, the host organization should require the submission by the sponsor of a Technology Control Plan (TCP) for every research project, product, service, funding opportunity, and online tool to the designated export compliance official. The TCP should not be confused with an information protection plan, which is required for computer access. The purpose of the TCP is to protect against an unauthorized transfer of export-controlled information. Also, the technical SME should provide support and participate in the process in the development of an appropriate TCP. A template example of a TCP is given in Appendix E. A reference guide for ensuring an effective export control and compliance program can be found in the Export Control Checklist (Appendix D).

What constitutes an effective Technology Control Plan (TCP)
A TCP ensures that appropriate controls are in place to minimize the risk of an improper transfer of export-controlled information. Development of this plan will require Export Compliance lead(s) to visit the facility where a foreign national will be working and determine areas of potential illegal transfer of export-controlled technology and conduct audits to ensure adherence to all aspects of TCP (See Appendix E).

This TCP applies to all elements that may be involved in the hosting or sponsoring of foreign persons. The TCP places specific requirements on sponsors and their supervisors, both of whom are responsible for taking all reasonable measures to prevent the disclosure of inappropriate information to foreign persons. Under this TCP, sponsors may only permit disclosure of information that is: unclassified, non-sensitive, and non-export-controlled; directly applicable to the tasks assigned to the foreign national; or has been approved for release to the public. Disclosure of other categories to a foreign person is considered an export that might require an authorization from either the Department of State or the Department of Commerce.

Training and Awareness

Staff who engage with foreign organizations and citizens should be required to take a minimum set of training modules including IT security, counterintelligence, and OPSEC every year. Additional training and informational awareness updates should be provided by the Team on a regular basis as part of the communication strategy. In-person reviews are a great opportunity to re-enforce training and awareness and continue to build cultural buy-in. Regular office hour sessions may be used to collect feedback from staff as well as answer any outstanding concerns.

The use of the ODNI Safeguarding Science Toolkit [5] provides staff with a collection of research security tools to help protect their research from intellectual property theft. The host organization should establish an internal website for safeguarding international science research security and a single point of team contact e-mail address.

12. Privacy and Inclusivity

A foundation of the organizational research security policy should be to preserve and protect privacy information to safeguard against xenophobia. At the same time, procedures must be established that promote inclusive opportunities for scientists to engage with other scientists.

13. Conclusion

The Framework is a guide for research security practitioners needing to develop a multi-disciplined assessment of research security risks unique to open scientific collaboration. Using strategic communication, and mission-focused methodologies, the implemented Framework provides transparency that encourages cultural buy-in of an organization's workforce by revealing how balanced security countermeasures can safeguard U.S. intellectual property and preserve the hard-earned credit for their research.

In summary, as shown in Table 9, the NIST Safeguarding Science Research Security Framework design is holistic, scalable, and adaptable to meet the different mission needs of the science and research community (e.g., USG, academia, and industry). The implementation of the Framework assists organizations, regardless of size or risk profile of activities, to apply the principles and best practices of a risk-balanced management approach to safeguarding international science and technology from undue foreign influence and interference while protecting the openness and integrity of the U.S. research ecosystem. Striking a balance between openness, security, and international collaboration and the methodologies and requirements for an integrated mission-focused research security program protects the openness and integrity of U.S scientific research.

Table 9. Implementation matrix for the safeguarding science research security framework

International Science • Promotes international collaboration • Enables cutting-edge research • Leverages resources • Promotes harmonized standards	**Research Security Focus Areas** • Fundamental research • Dual-use technologies • Critical and emerging technologies • Standards • Proprietary/defense	**Key Contributors** • USG research agencies • USG intelligence community • USG Executive Branch • Universities • Industry
Risks • U.S. National Security • U.S. Economic Security • U.S. Researchers	**Safeguarding U.S. Research Ecosystem** • Employ a balanced multi-discipline methodology • Understand the Science (fundamental, applied, military-civil fusion, patents, standards) • Determine risk and benefit • Apply non-intrusive countermeasures	**Changing the Culture** • Understanding the why • Communication • Assessment tools & resources • Awareness Training • Subject matter expert buy-in & accountability
Research Security • Balanced approach • Extramural programs • Intramural programs • Policies • Resources tools (e.g., ORCID, CSET CITADEL, Google Scholar, ASPI, etc.)	**Consideration** • Integrate research security/insider Threat/Operations Security • Proprietary funded research (disclosure authority, enhanced security) • Understanding competitor collection strategy and target technologies	**Information Sources** • Team composition • Subject matter expertise • Open source • Intelligence community

References

[1] The Office of the President, *National Security Presidential Memorandum - 33 on United States Goverment-Supported Research and Development National Security Policy,* The White House, 2021.

[2] National Science and Technology Council, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development,* Subcommittee on Research Security, Joint Committee on the Research Environment, 2022.

[3] National Science and Technology Council, *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise,* Subcommittee on Research Security, Joint Committee on the Research Environment, 2021.

[4] Director of the National Counterintelligence and Security Center, *National Security Presidential Memorandum/NSPM-28, The National Operations Security Program, 13 January 2021,* Washington DC, 2021.

[5] Office of the Director of National Intelligence, *Safeguarding Science,* The National Counterintelligence and Security Center, [Online]. Available: https://www.dni.gov/index.php/safeguarding-science. [Accessed 15 June 2023].

[6] Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Emplyees and Contractors,* Chief Security Officer, 2004.

[7] Department of Commerce, Office of Security, *Department Administrative Order (DAO) 207-12, Foreign National Visitor and Guest Access Program,* Department of Commerce, 2021.

[8] National Institute of Standards and Technology, *About NIST,* NIST, 11 January 2022. [Online]. Available: https://www.nist.gov/about-nist. [Accessed 20 April 2023].

[9] R. Fedasiuk, *The China Scholarship Council: An Overview,* Center for Security and Emerging Technology, 2020.

[10] U.S. Department of State Bureau of Consular Affairs, *Travel Advisories,* [Online]. Available: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/. [Accessed June 2023].

[11] U.S. Department of State, *Military-Civil Fusion and the People's Republic of China,* [Online]. Available: https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf. [Accessed June 2023].

[12] 117th Congress, *Public Law 117-183: SBIR and STTR Extension Act of 2022,* 117th Congress, 2022.

[13] National Science and Technology Council, *Critical and Emerging Technologies List Update,* Executive Office of the President of the United States, 2022.

[14] International Organization for Standardization, *Guide 73: Risk management - Vocabulary (ISO Guide 73:2009),* 2009.

[15] K. Stine, R. Kissel, W. C. Barker, J. Fahlsing and J. Gulick, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories,* National Institute of Standards and Technology, Gaithersburg, 2008.

[16] C. N. Saha and S. Bhattacharya, Intellectual property rights: An overview and implications in pharmaceutical industry, *Journal of Advanced Pharmaceutical Technology & Research,* vol. 2, no. 2, pp. 88-93, 2011.

[17] U.S. Department of Defense, *DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions,* 2025. [Online]. Available: https://basicresearch.defense.gov/Programs/Academic-Research-Security/. [Accessed August 2025].

[18] Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council, *Critical and Emerging Technologies List Update,* Executive Office of the President of the United States, 2022.

[19] Department of Commerce International Trade Administration, *U.S. Export Regulations,* [Online]. Available: https://www.trade.gov/us-export-regulations-0. [Accessed June 2023].

[20] Code of Federal Regulations, *Title 22 Foreign Relations, Subchapter M International Traffic in Arms Regulations,* National Archives, 2023.

[21] U.S. Department of Agriculture, *Departmental Regulation 4600-003: USDA Defensive Counterintelligence and Insider Threat Programs,* Washington, D.C., 2021.

[22] Office of the Federal Register (OFR), *Executive Order 12333 -- United States intelligence activities,* National Archives, 1981.

Appendix A. Additional Research Security Resources

J. Arterburn, *New Data for New Approaches to Research Security,* May 04, 2022. [Online]. Available: https://researchservices.upenn.edu/wp-content/uploads/2022/04/China-Initiative-C4ADS.pdf

R. Lester *et al.*, *University Engagement with China: An MIT Approach (Final Report),* MIT China Strategy Group, Nov. 2022. [Online]. Available: https://global.mit.edu/wp-content/uploads/2022/11/FINALUniversity-Engagement-with-China_An-MIT-Approach-Nov2022.pdf

M. J. Vernick and M. A. Thompson, *Anatomy of a Foreign Influence Investigation,* May 2022, [Online]. Available: https://researchservices.upenn.edu/wp-content/uploads/2022/04/Anatomy-of-a-Foreign-Influence-Investigation.pdf

Congressional Research Service, *Federal Scientific Integrity Policies: A Primer,* R46614, Nov. 2022. Accessed: Apr. 13, 2023. [Online]. Available: https://www.congress.gov/crs_external_products/R/PDF/R46614/R46614.8.pdf

Council on Government Relations, *Federal Focus on Inappropriate Foreign Influence on Research: Practical Considerations in Developing an Institutional Response,* 2021. Accessed: Apr. 17, 2023. [Online]. Available: https://www.cogr.edu/sites/default/files/COGR%20Foreign%20Influence%20Practical%20Considerations%20-%20Aug%202021%20%281%29.pdf

G. Long, *Research Program on Research Security,* JSR-22-08, Mar. 2023. [Online]. Available: https://nsf-gov-resources.nsf.gov/2023-03/JSR-22-08%20NSF%20Research%20Program%20on%20Research%20Security_03152023_FINAL_1.pdf

U.S. Senate, Committee on Homeland Security and, *S. Rept. 117-282 - SAFEGUARDING AMERICAN INNOVATION ACT,* legislation, 2022. Accessed: Apr. 13, 2023. [Online]. Available: https://www.congress.gov/117/crpt/srpt282/CRPT-117srpt282.pdf

F. Bekkers, W. Oosterveld, and P. Verhagen, *Checklist for Collaboration with Chinese Universities and Other Research Institutions.* The Hague Centre for Strategic Studies, 2021. [Online]. Available: https://hcss.nl/wp-content/uploads/2021/01/BZ127566-HCSS-Checklist-for-collaboration-with-Chinese-Universities.pdf

Canada, *National Security Guidelines for Research Partnerships Risk Assessment Form.* 2023. [Online]. Available: https://science.gc.ca/site/science/sites/default/files/attachments/2023/risk_assessment_form_ISED-ISDE3832E.pdf

Canadian Security Intelligence Service, *Safeguarding your Research Checklist,* Government of Canada, 2022. [Online]. Available: https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/csis-and-research-security#2

Government of Canada, *National Security Guidelines for Research Partnerships,* Government of Canada, 2022. [Online]. Available: https://science.gc.ca/site/science/sites/default/files/attachments/2023/national_security_guidelines_for_research_partnerships.pdf

New York University, *Investigator Initiated Documents Required to Participate in Federally Funded Research.* Accessed: Apr. 17, 2023. [Online]. Available: https://www.nyu.edu/research/research-policies/research-and-foreign-engagement/investigator-initiated-documents-required-to-participate-in-fede.html

Australian Government, Department of Education, *Guidelines to Counter Foreign Interference in the Australian University Sector,* Accessed: Apr. 18, 2023. [Online]. Available: https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector

I. d'Hooghe and J. Lammertink, *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology,* LeidenAsiaCentre (of Leiden University, the Netherlands), Nov. 2022. [Online]. Available: https://www.security-relevant-research.org/publication-leiden2022/

OECD Science, Technology and Industry Policy Papers, *Integrity and Security in the Global Research Ecosystem,* 130, Jun. 2022. [Online]. Available: https://www.oecd.org/en/publications/2022/06/integrity-and-security-in-the-global-research-ecosystem_2bd8511d.html

C. Shillum, S. Sadler, and J. Petro, *ORCID Poised to Support Research Institutions in New Era of Public Access and Research Security,* Accessed: Apr. 17, 2023. [Online]. Available: https://info.orcid.org/orcid-poised-to-support-research-institutions-in-new-era-of-public-access-and-research-security/

Appendix B. Definitions

Australia Strategic Policy Institute (ASPI) China Defense University Tracker
The China Defense Universities Tracker is a database of Chinese institutions engaged in military or security-related science and technology research. It is a tool that enables universities, governments, the business community, and scholars to conduct due diligence as they conduct business with China.

Basic Research
Experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts [17].

Center for Security and Emerging Technology (CSET)
A policy research organization within Georgetown University's Walsh School of Foreign Service, CSET provides decision-makers with data-driven analysis on the security implications of emerging technologies.

CHIPS and Science Act
The CHIPS and Science Act is a federal statute signed into law on August 9, 2022 that will boost American semiconductor research, development, and production, ensuring U.S. leadership in the technology that forms the foundation of everything from automobiles to household appliances to defense systems.
https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

Clarifications
Clarifications are any additional questions or requests for information that arise during the initial risk determination. This can include additional information that may reduce the risk determination, missing information, or information that conflicts with or cannot be validated against Findings. Requests for clarification can be a useful part of establishing an open dialog and transparent process.

Conflict of Interest
According to the 18 U.S.C.§208, a conflict of interest is a personal interest or relationship that conflicts with the faithful performance of official duty. – Situation in which an individual, or the individual's spouse or dependent children, has a significant financial interest, or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research [2].

Conflict of Commitment
A conflict of commitment is a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment [2].

Consolidated Screening List
The Consolidated Screening List (CSL) is a list of parties for which the United States Government maintains restrictions on certain exports, reexports, or transfers of items. Below, under "Tools" are links to the CSL search engine, downloadable CSL files, and the CSL Application Programming Interface (API), all consisting of the consolidation of multiple export screening lists of the Departments of Commerce, State, and Treasury.
https://www.trade.gov/consolidated-screening-list

Covered Individual
An individual at an extramural research institution who, as designated by the extramural research institution, contributes significantly to the design or execution of a research and development project, and who is considered essential to the successful performance of the research and development project. Covered individuals include those listed as key personnel in fundamental research project proposals (e.g., the principal investigator or co-principal investigator) [17].

Critical and Emerging Technology
Critical and emerging technologies (CETs) are a subset of advanced technologies that are potentially significant to U.S. national security [18].

Department of Commerce Foreign Access Management (FAM)
The DOC FAM (DAO 207-12) sets forth Department of Commerce (DOC or Department) policies and procedures for foreign national visitor and guest access to Department facilities, resources and activities. The FAM acknowledges the increased diversity of foreign participation and the need for updated control measures beyond foreign visitor control to manage present day risks associated with physical and logical access to the Department's facilities and resources.

Export Administration Regulations (EAR)
The Export Administration Regulations govern the export and re-export of some commodities, software, and technology [19].

Export Control
Export Controls are Federal Laws and regulations that govern the transfer or disclosure of goods, technologies, software, services, and funds originating in the U.S. to persons or entities in foreign countries or non- U.S. persons even if located in the U.S.

Findings
Findings are the fact-based Indicators or Warnings that inform the risk determinations for each principal category. Subsequently, Findings drive the first risk determination. Findings must be relevant to the scientific field or technology under consideration. Consideration for the Science and Technology drives the research security review process.

Foreign Country of Concern
The term foreign country of concern means:

(a) A country that is a covered nation (as defined in 10 U.S.C. 4872(d)); and

(b) Any country that the Secretary, in consultation with the Secretary of Defense, the Secretary of State, and the Director of National Intelligence, determines to be engaged in conduct that is detrimental to the national security or foreign policy of the United States. https://www.federalregister.gov/documents/2023/03/23/2023-05869/preventing-the-improper-use-of-chips-act-funding

Foreign Talent Recruitment Program
Effort organized, managed, or funded by a foreign government, or a foreign government instrumentality or entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position).

Host Organization
Organization receiving visiting scientist/researcher.

International Traffic in Arms Regulation (ITAR)
The International Traffic in Arms Regulations (ITAR) (22 CFR parts 120-130) governs the manufacture, export, and temporary import of defense articles, the furnishing of defense services, and brokering activities involving items described on the USML (ITAR section 121.1) [20].

International Trade Administration Consolidated Screening List (ITA CSL)
The Consolidated Screening List (CSL) is a list of parties for which the United States Government maintains restrictions on certain exports, reexports, or transfers of items. Below, under "Tools" are links to the CSL search engine, downloadable CSL files, and the CSL Application Programming Interface (API), all consisting of the consolidation of multiple export screening lists of the Departments of Commerce, State, and Treasury.

Malign Foreign Talent Recruitment Program
Foreign government-sponsored talent recruitment program operated with the intent to import or otherwise acquire from abroad, sometimes through illicit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government.

Malign Foreign Talent Placement Program
A program where the foreign country (often the government) targets the technology and location for a NTIC to acquire intellectual property to fill an identified knowledge gap to foster the goals of achieving national military and economic superiority. This program is implemented through foreign challenges, fellowships, and scholarship awards.

Military-Civil Fusion Technology: Military-Civil Fusion (MCF)
MCF is an aggressive strategy to enable the development of the most technologically advanced military in the world through research and development efforts, as well as by acquiring and diverting the world's cutting-edge technologies – including through theft – to achieve military dominance.

Mitigations
Mitigations are intended to reduce the severity or the effects of identified research security risks. Within the context of a risk-balanced approach, a mitigation is a targeted required action that is made at the individual research security review level on a case-by-case basis. While intended to reduce research security risk, mitigations can only reduce the level of the initial risk determination by one level. The introduction of mitigations cannot negate risk unless the cause for mitigation is completely removed.

Non-Intrusive Countermeasures
An action associated with the employment of a single or set of mutually supporting security access control measures collaboratively designed with the Principal Investigator to mitigate known or anticipated threat or vulnerability to an emerging data or technology set resident within the science and research environment having minimal impact upon research project or program objectives.

Non-Title 50 (NT-50)
Refers to those Federal departments and organizations who authorities derive from portions of United States Code (U.S.C.) other than Title 50 or E.O. 12333, which addresses U.S. intelligence activities. NT50s are involved in many activities that affect national security, such as conducting foreign affairs, combating pandemic diseases, halting illicit trafficking, conducting scientific and medical research, regulating finance, commerce, and transportation, and protecting food, water, and nuclear infrastructures (adapted from [21]).

Non-Traditional Collector
Individuals whose primary profession is not intelligence collection but who collect sensitive U.S. technologies and information on behalf of foreign adversaries. (paraphrased from: https://www.fbi.gov/file-repository/counterintelligence/china-case-example-insulation-2019.pdf/view)

Persistent Digital Identifier
A digital identifier that is globally unique, persistent, machine resolvable and processable, and has an associated metadata schema. Consistent with NSPM-33, digital persistent identifiers for individuals are used to disambiguate and identify an individual person.

Principal Investigator
A Principal Investigator or PI is the individual responsible for the preparation, conduct, and administration of a research grant, cooperative agreement, training or public service project, contract, or other sponsored project.

Recommendations
Recommendations are not required actions but are non-binding suggested courses of action for an improvement to the research security risk for the entity being reviewed. A Recommendation does not impact the risk determination but rather is intended as a long-term effort to suggest research security-related improvements.

Research Associate
Individuals who have a formal affiliation with the organization but are not employees of the organization to perform research on a specified topic. Research associates may be either foreign or domestic.

Research Integrity
The use of honest and verifiable methods in proposing, performing, and evaluating research; reporting research results with particular attention to adherence to rules, regulations, and guidelines; and following commonly accepted professional codes or norms.

Research Security
Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference [2].

Safeguarding International Science
A risk-balanced approach to implementing a research security program that balances open scientific international collaboration while safeguarding the U.S. research ecosystem. Both objectives are intrinsic to research security and integrity initiatives.

State Sponsor of Terrorism
Countries determined by the Secretary of State to have repeatedly provided support for acts of international terrorism (see https://www.state.gov/state-sponsors-of-terrorism/).

User Activity Monitoring (UAM)
The technical capability to observe and record the actions and activities of an individual, at any time, on any information system, platform or device accessing U.S. Government information.

Appendix C. Review Form Templates

Research Associate Appointment Review Form

Foreign Travel Review Form

Products, Services, and Software Tools Review Form

Funding Opportunities Review Form

Research Associate Appointment Review Form			
(To be completed by Host or Supervisor)			
Information for: (Name: First, Middle, Last)			
Organization Unit	**Organization Group**	**Agreement Start Date**	**Agreement End Date**

Citizenship(s) (list all)	
FNR Employer (Organization Name)	
Sponsor (Funding organization if different from Employer)	
Universities attended and dates (Undergraduate and graduate)	
Scholarships/Funding from non-US sources [Name of Scholarship and Funding Organization (e.g., foreign talent recruitment programs, foundations, government sponsored scholarships)]	
Affiliations (Any other organization with whom the FNR has a formal relationship or obligation)	
FNR is a U.S. Lawful Permanent Resident (LPR)	☐Yes ☐No
If extension, visa type **Visa sponsor**	

Host/Sponsor Information	
NIST Host Name	
NIST Host Division name and number	
NIST Host Division Chief	
NIST Host Affiliations/external appointments • *All sources of **current and pending support*** • *All current **professional appointments** outside of organization* • *Foreign collaborations in major facilities*	
Number of FNRs assigned to the Host (may not exceed 5)	
Date of completion of most recent Host/Sponsor Counterintelligence Training	
Origin of Recruitment (how did the host identify the FNR)	

Project Information	
Is the FNR supported by and subject to the terms and conditions of a funding agreement with a United States university or a United States company? If yes, agreement type and number	☐Yes ☐No
Will the FNR or the Project be supported by any external entity, such as another USG agency, foreign entity, or commercial/proprietary source funding? Identify all sources of support and, if external source, provide written confirmation that the external source (Program Manager) agrees to this appointment.	
Site access – Buildings and Rooms	
Does the research involve, U.S. national security, export controlled, proprietary or other controlled information?	☐Yes ☐No
Technology Control Plan Reviewed and approved by Export Control Officer?	☐Yes ☐No please attach
Project Title/Subject	
Research Area (e.g. Quantum, Bio, AI, 5G etc)	
Project Plan/Job Description	
Benefit to Organization	
Fundamental Research Plan Insert broad base programmatic research and the specific focus of the research in a scientific journal abstract style (one paragraph) Add a statement that confirms that the project/program scope is limited to fundamental research	

Are there any known military/civilian fusion technology applications that can be derived from this research? If yes, please explain If no, please explicitly state as such and why	☐Yes ☐No
Are there any possible outcomes of this research that are patentable? If yes, please identify (title) and status	☐Yes ☐No
Site/resource access (work hours):	

TO BE COMPLETED BY EXPORT CONTROL OFFICER	
Foreign Party Affiliations	
RISK Level Determination	
Export Control/Proprietary Information	
Comments:	

REVIEW BOARD FINDINGS	
Comments:	

Review of request result

Reviewers	Approve/Disapprove	Comments	Date
Host/Sponsor			
Supervisor			
Research Security Team			
Decision			

Foreign Travel Review Form (Virtual and Physical) Submit to research security team at least 3 days prior to the date needed to commit to travel	
Staff Name/Organizational Department	
Event type: (e.g., International Conference/Workshop/ Collaboration/Presentation/ Other?	
Purpose Statement: (what is the role of the participant? spell out all acronyms)	
If presenting, Title and Abstract	
Name of Event and Event Website information: (If no website available, list "no website")	
Event host organization(s)/sponsor(s)	
Meeting Dates and/or Attendance Dates:	
Benefit to Organization Statement: (please spell out all acronyms)	
Foreign Funding support (e.g., Is the registration fee being waived?)	
Please note any known mil/civ applications [are there are any applications of the research that the staff member plans to present that might have military or civil (commercial) applications?]	
Research funding source (Is the funding for the research being presented internal or external and does the external funding have any concerns with presenting the results to a foreign audience)	

Research Security Review Team finding (concur or non-concur):

Date of review finding:

Products, Services, and Software Tools Review Form (to be completed by relevant internal office within the organization)	
Name of Product, Service, or Software Tool	
Description / Use Purpose	
Internal Technical Point of Contact	
Company and Country requesting purchase	
Industry Focus (provide URL if possible)	
Review Findings (to be completed by Research Security Review Team)	
Are there any known military/civil fusion technology applications that can be derived from this Product/service?	
Consolidated Screening / Entity List https://www.trade.gov/data-visualization/csl-search	
Export License Required? (If so, cite ECCN and method of control)	
Request matches Company's Technology needs (y/n)	
Risk level (Very High, High, Medium, Low)	
Research Security Review Team finding (concur or non-concur) **Date**	

Funding Opportunities Review Form	
Applicant Information (to be completed by Funding Organization)	
Applicant Legal Name	
Applicant Address (Street, City, State, Zip Code, Country)	
Technology Type (Brief Description of Project, e.g., AI, Quantum, Biology, etc.)	
Key Personnel Name(s) and Title(s)	
Company URL (if possible)	
Review Findings (to be completed by Research Security Review Team)	
Are there any foreign financial obligations that may create undue foreign influence or interference?	
Are there any known military/civil fusion technology applications that can be derived from this proposal?	
Consolidated Screening / Entity List https://www.trade.gov/data-visualization/csl- search	
Are there any conflicts of interest or commitment?	
Risk level (Very High, High, Medium, Low)	
Reason for Determination	
Recommendation (may include request for further information or discussion)	
Date Reviewed	

Appendix D. Review Checklists

General Operations Checklist

Research Associate Appointment Checklist

Foreign Travel Checklist

Foreign Collaboration Checklist

Foreign Request for Products, Services and Software Tools Checklist

Extramural Funding Opportunities Checklist

Export Compliance Checklist

NIST IR 8484 Research Security General Operations Checklist (8484 GOC)

Performing research security reviews of grant proposals is critical to protecting the U.S. supply chain and the research ecosystem of emerging semiconductor and microelectronic technologies that are essential to U.S. economic and national security.

Research Security Reviews consider a myriad of key questions that apply to covered institutions and covered individuals. Answers to key questions are obtained through open-source intelligence (OSINT) as well as information provided by the funding opportunity applicant. Table 1 is a NIST IR 8484-derived general operations checklist (8484 GOC). This is a consolidated list (non-inclusive) of the key questions extending across the five review categories (researchers, travel, products & services, funding opportunities, and publications & collaborations) and the five checklists included in NIST IR 8484 Appendix D. The use of 8484 GOC addresses the research-security criteria contained within federal initiatives (NSPM-33, CHIPS & Science Act, SBIR/STTR Due Diligence Act).

Table 1. NIST IR 8484 Research Security Framework General Operations Checklist (8484 GOC). A non-inclusive list of key research security questions for reviewing researchers, foreign travel, products & services, funding opportunities, and publications & collaborations.

NIST IR 8484 Research Security Framework General Operations Checklist (8484 GOC)		
Institution	**Individual**	**Both**
FOCI – Foreign Ownership Control and Influence	Conflicts of Interest	ITA Consolidated Screening / Entity List
Foreign Obligations	Conflicts of Commitment	Capabilities match request
Cybersecurity	Foreign Education	Military / Civil applications
Data management	Foreign Talent Recruitment Programs (Benign and Malign)	
Export Control and Compliance	Malign foreign affiliations (e.g., Universities, Confucius Institutes, Organizations, Professional Memberships, Scholarships, Awards, etc.)	
Venture Capital	Position sensitivity - Access (CUI / Intellectual Property / Technology)	
Research Security Plan / Program	Foreign publications/Patents	
	Scholarships / Awards	
	Professional Associations	
	Foreign travel (e.g., conferences, symposiums, and meetings)	

A Research Security Review is a collaborative decision-making process between the Team and organizational management consisting of a risk/benefit recommendation by the Team to organizational management for a final risk determination. The composite analysis of the information acquired and assessed during a research security review results in a risk-balanced determination of low, medium, or high risk contained within the Research Security Review Form. A no risk determination is impractical as achieving a no risk security posture is unrealistic and can be deceptive of underlying risk to customers, asset owners, and research security practitioners. A low-risk determination concludes that the risk is acceptable and that the benefits to the organization clearly outweigh the risk. A medium risk determination concludes that an identified risk exists, and that the risk can be mitigated through the deployment of available security countermeasures to achieve an acceptable risk/benefit determination. A high-risk determination concludes that a targeted collection risk exists, and that the deployment of available security countermeasures may be insufficient to achieve an acceptable risk/benefit determination resulting in a rejection of the grant application. Targeted high-risk collection threats may require validation from non-OSINT sources.

FOREIGN NATIONAL ASSOCIATE RESEARCHER CHECKLIST

A Research Security program creates an integrated risk-balanced approach to safeguard the U.S. science & technology community from undue foreign interference. Success is through maintaining an inclusive culture that promotes international science while safeguarding the research ecosystem.

SPECIFIC CONSIDERATIONS

Consideration is given to the potential Foreign National Associate (FNA) research skills and their benefit to the organizational mission, where the benefit must outweigh the risk.

Key Areas of Interest
FNA Foreign Affiliations: Risk can exist when a candidate FNA is affiliated (e.g., postgraduate degree, scholarship, grants, current research, active society membership or malign foreign talent recruitment program).
FNA Recruitment: Determining the FNA recruitment occurred is critical. Did the FNR initiate the request or was the position filled through open competition (preferred).
Funding Source: Funding sources may include your own organization, external USG organization (e.g., NSF, NIH, DOE, DARPA), university, commercial, and/or foreign scholarships. Foreign grants or scholarships can be affiliated with malign talent recruitment programs and must be reviewed.
Fundamental Research and Project Plan: The fundamental research and project plan explains the project scope and describes the fundamental research, critical and emergent technologies, possible applications.
Benefits to the Organization: The FNR benefit is to the organizational mission and not the PI.
Technology Control Plan (TCP): Organizations possess intellectual property and technologies that may require protection. A TCP assesses every project/program for export, transfer or disclosure controls on any data, equipment, or software and allowable access. Ensures compliance with USG requirements (e.g., EAR/ITAR).
Military-Civil Fusion (MCF): MCF is a strategy where select competitor nations pursue the collection of critical emerging technologies (CETs) intellectual property through lawful or illicit means to advance their economic and national security objectives. Assessment (w/the Principal Investigator) of CETs within the research (including fundamental research) which may have dual-use applications is required.
Patentable Outcome: Patents and potential patents are inherently linked to the potential commercial (dual-use) application of a CET. The PI is likely more apt to consider patent applications as a routine outcome of their research. A patentable potential is reason to infer that an increased MCF target.
Facility Access Control: Access control is part of a viable research security program. Perimeter and point of entry controls provide security in-depth but should scale to meet the risk level. Contiguous research spaces should be considered to determine access risk to other intellectual property or proprietary research.

BEST PRACTICES CHECKLIST

- ☐ Do the skills of the FNA match the programmatic research?
- ☐ Did you determine the FNA affiliations, both direct and indirect?
- ☐ Did you determine how the FNA was recruited?
- ☐ Did you determine any funding sources?
- ☐ Did you determine export control issues and articulate them in the TCP?
- ☐ What are the military-civil fusion technology applications, especially critical and emerging technologies?
- ☐ Do the access controls (logical and physical) in place mitigate the risk level?
- ☐ Do the Benefits to the Organization outweigh the Risk?

FOREIGN TRAVEL CHECKLIST

With the ever-changing nature of the virtual and physical work environment and increasing diversity of the technology collection threat directed at the U.S. scientific research community, it is increasingly important to protect yourself and your organizatioin from becoming a target.

SPECIFIC CONSIDERATIONS

Participation in foreign-sponsored virtual travel (e.g., teleconferences) and physical travel may support mission objectives, but it may provide competitors or adversaries an opportunity to target information that, if lost, could harm, or disrupt mission-focused science programs. Practicing Operations Security (OPSEC) can help you identify critical information and protect it from unwanted loss or compromise.

Points for Consideration for When Virtually or Physically Traveling to a Foreign Country
General Compliance: ☐ Comply with all organizational policies for review/approval of official travel (virtual and physical), pre-publication/public release of papers or presentations, and possible export licensing requirements. ☐ Direct questions to your supervisor or your Research Security Team
Cybersecurity: ☐ Ensure all electronic communication with foreign entities is conducted via official channels using virtual private networks to mitigate cyber-security risks. ☐ Be mindful of links, attachments, or downloads received (especially for virtual travel), including “Apps” or plugins, which are often written by unknown third parties, and can be used to access or inject malicious software into your system or networks. ☐ Contact your IT Security Officer to ask questions or obtain additional guidance.
OPSEC: ☐ Know your boundaries. Limit your discussions to the scope of the authorized topic. ☐ Do not discuss personal or sensitive information (e.g., social media activity, friends, family, or work-related information such as coworkers, research projects, or organizational structure). ☐ Sanitize your space before virtually connecting with foreign entities to remove or obscure visible badges, credentials, pictures, diplomas, awards, marker boards, org-charts, etc.
Reporting: Report the following to your security office. ☐ If you have any direct involvement or affiliation with the sponsoring foreign entity or organization that may imply a conflict of interest or commitment with your official duties. ☐ Any attempts by a foreign entity to engage with you in any capacity unassociated with the travel (e.g., social encounter, social media friend request, or email request for assistance) ☐ Any attempts by a foreign entity to obtain information from you that exceeds the authorized scope of your presentation before, during, or after the travel. ☐ Any activity that you consider to be questionable or suspicious.

FOREIGN COLLABORATION CHECKLIST

A Research Security program creates an integrated risk-balanced approach to safeguard the U.S. science & technology community from undue foreign interference. Success is through maintaining an inclusive culture that promotes international science while safeguarding the research ecosystem.

SPECIFIC CONSIDERATIONS

Consideration of the collaboration type (e.g., bilateral or multinational) and organization(s) enables a Benefit versus Risk analysis. For bilateral collaborations, the risk of intellectual property theft may occur if the organization is targeting a military-civil technology gap.

Key Areas of Interest
Collaboration Participants: Those from countries of concern should be reviewed with respect to technology gaps and interests the requesting organization. Determine if the requesting organization is a malign foreign talent recruitment program. A multinational collaboration is preferred.
Technology Type: Determine if this is a critical emerging technology and considered a technology target of a country of concern. The research should align with the home organization scientific mission.
Benefits to the Organization: The benefit is to the home organization science mission and not the PI. All fundamental research outcomes will be published in the public domain.
Funding Source: Funding sources may include your own organization, external USG organization (e.g., NSF, NIH, DOE, DARPA), university, commercial, and/or foreign scholarships. A review of foreign grants or scholarships of the requestor to determine align talent recruitment programs affiliation is needed.
Technology Control Plan (TCP): Organizations possess intellectual property and technologies that may require protection. A TCP assesses every project/program for export, transfer or disclosure controls on any data, equipment, or software and allowable access. Ensures compliance with USG requirements (e.g., EAR/ITAR).
Military-Civil Fusion (MCF): MCF is a strategy where select competitor nations pursue the collection of critical emerging technologies (CETs) intellectual property through lawful or illicit means to advance their economic and national security objectives. Assessment (w/the Principal Investigator) of CETs within the research (including fundamental research) which may have dual-use applications is required.
Patentable Outcome: Patents and potential patents are inherently linked to the potential commercial (dual-use) application of a critical and emerging technology. The PI is likely more apt to consider patent applications as a routine outcome of their research. A patentable potential is reason to infer that an increased MCF target.
Publication: For the country of concern author(s), a risk level determination is needed of the author's organization at the time of publication and whether the author(s) is affiliated with a malign foreign talent recruitment program. If the research outcomes are a critical emerging technology, then new technology outcome may need protection and may require export control. Research funding should be determined as well.

BEST PRACTICES CHECKLIST

- ☐ Collaboration request is bilateral or multinational?
- ☐ Any funding/affiliation alignments with a malign foreign talent recruitment program?
- ☐ Will all fundamental research outcomes be published in the open domain?
- ☐ Did you determine export control issues and articulate them in the TCP
- ☐ What are the military-civil fusion technology applications, especially critical and emerging technologies?
- ☐ Do the Benefits to the Organization outweigh the Risk?

FOREIGN REQUEST FOR PRODUCTS, SERVICES, AND SOFTWARE TOOLS CHECKLIST

A Research Security program creates an integrated risk-balanced approach to safeguard the U.S. science & technology community from undue foreign interference. Success is through maintaining an inclusive culture that promotes international science while safeguarding the research ecosystem.

SPECIFIC CONSIDERATIONS

Consideration of the requests from a country of concern organization should be reviewed to recognize any potential military-civil technology application advancement that may occur. Additionally, all requests must be checked for export control license restrictions.

Key Areas of Interest
Product, services, or software tool: Requests from a country of concern organization should be reviewed to recognize any potential military-civil technology application advancement that may occur. Additionally, all products and services requests from a foreign organization must be checked for export control license restrictions.
Requesting Foreign Organization: Requests from countries of concern should be reviewed with respect to technology gaps and interests of the requesting organization. Determine if the requesting organization is part of a malign foreign talent recruitment program.
Export Control: Certain products, services and software tools may require protection and/or review prior to its delivery to ensure compliance with U.S. law and regulatory requirements (e.g., EAR/ITAR).
Sanctions: Some countries (e.g., State Sponsors of Terrorism) may have sanctions listed in the DOC ITA Consolidated Screening List. Determine any sanctions restricting business with a requesting country.
Military-Civil Fusion (MCF): MCF is a strategy where select competitor nations pursue the collection of critical emerging technologies (CETs) intellectual property through lawful or illicit means to advance their economic and national security objectives. Assessment (w/the Principal Investigator) of CETs within the research (including fundamental research) which may have dual-use applications is required.

BEST PRACTICES CHECKLIST

- ☐ Does the requesting organization have alignment with a malign foreign talent recruitment program?
- ☐ Did you determine any export control?
- ☐ Did you determine any sanction issues?
- ☐ What are the military-civil fusion technology applications, especially critical and emerging technologies?

EXTRAMURAL FUNDING OPPORTUNITIES CHECKLIST

A Research Security program creates an integrated risk-balanced approach to safeguard the U.S. science & technology community from undue foreign interference. Success is through maintaining an inclusive culture that promotes international science while safeguarding the research ecosystem.

SPECIFIC CONSIDERATIONS

The funding opportunity type is mission specific to the requesting organization. This may include the following: grant, cooperative agreement, challenge, or other. USG funding opportunities may include specific foreign engagement requirements and restrictions.

Key Areas of Interest
Current and Pending Support: Determines potential conflict of interest and/or conflicts of commitment. Assists in identifying attachments to malign foreign talent recruitment programs and malign foreign talent placement programs. Affiliations include any past or present organization (foreign and domestic) with whom the associate has a formal relationship or obligations (e.g., universities, scholarships, professional societies, foreign talent recruitment programs. Applies to both the requesting organization and the Principal Investigator (PI).
Financial: Applies to an organization's financial business. Financial ties with a country of concern may be subject to specific USG requirements and restrictions. Collecting financial information is critical to a potential intellectual property targeting either through ownership or business contractual requirements. Those potential conflicts with monetary support require an increase scrutiny and an intellectual property risk determination.
Technology Control Plan (TCP): Organizations possess intellectual property and technologies that may require protection. A TCP assesses every project/program for export, transfer or disclosure controls on any data, equipment, or software and allowable access. Ensures compliance with USG requirements (e.g., EAR/ITAR).
Military-Civil Fusion (MCF): MCF is a strategy where select competitor nations pursue the collection of critical emerging technologies (CETs) intellectual property through lawful or illicit means to advance their economic and national security objectives. Assessment (w/the PI) of CETs within the research (including fundamental research) which may have dual-use applications is required.
Intellectual Property: Patents and potential patents are inherently linked to the potential commercial (dual-use) application of a CET. The PI is likely more apt to consider patent applications as a routine outcome of their research. A patentable potential is reason to infer that an increased MCF target.
Logical Access Control: Requesting organization should follow the NIST Cybersecurity Framework. Remote access to an organization's network should be tightly controlled and monitored. Digital intellectual property should be categorized and protected via authorized networks and personnel only.

BEST PRACTICES CHECKLIST

- ☐ Did you identify any potential conflicts of interest or commitment?
- ☐ Did you determine funding / affiliation alignments with a malign foreign talent recruitment program?
- ☐ Did you determine if there are any foreign financial concerns?
- ☐ Did you determine any export control or intellectual property issues?
- ☐ What are the military-civil fusion technology applications, especially critical and emerging technologies?
- ☐ Do the logical access controls in place mitigate the risk level?
- ☐ Do the Benefits to the Organization outweigh the Risk?

EXPORT COMPLIANCE AND CONTROLS CHECKLIST

Program Managers can use this checklist to ensure an effective export compliance and controls program. Implementing the below points for consideration helps create a culture of security that protects research as well as the individuals concerned, whether they are U.S. Citizens, U.S Persons, or foreign guests. The export compliance and controls program are the mechanism within an organization that provides checks and safeguards at key steps in program development and implementation, to help manage international activities to U.S. laws and regulations.

SPECIFIC CONSIDERATIONS

To ensure the long-term success of an export compliance program, a subject matter expert (SME) on all matters related to export control and international technology transfer should be appointed within an organization. The SME and all related staff should maintain an up-to-date knowledge of U.S. laws and regulations while considering the following points when creating and maintaining an effective program and how it fits into the overall research security for the organization.

Points for Consideration for an Effective Export Control Program
Management Commitment: First and foremost, has the Senior/Director level management approved a policy/directive that outlines the export compliance responsibilities for their organization? Does the policy/directive communicate that export compliance requires a proactive, organization-wide commitment that includes all levels, and that each employee plays a role in securing the integrity of the system?
Risk and Asset Management: What is the risk to your organization? The reality of the global competitive environment today is such that both nation states and non-state actors compete for technical advantage to advance their national and economic security objectives. What do you have- item, software, technology, project, etc.- that requires protection per the EAR or ITAR? Remember that compliance requirements might change per guest researcher citizenship.
Training: Does your organization provide adequate resources and opportunities- both live and virtually- for export compliance training at various levels? Providing training that is tailored to specific research where the audience is familiar and already interested creates a more engaging environment.
Audits and Recordkeeping: Do you have an up-to-date Technology Control Plan (TCP) in place? A TCP is the document that ensures appropriate controls are in place prior to the commencement of the FNA visit to minimize the risk of an improper transfer of export-controlled information. The TCP also places specific requirements on sponsors and their supervisors who are responsible for taking all reasonable measures to prevent the disclosure of inappropriate information to foreign persons.

BEST PRACTICES CHECKLIST

- ☐ Have you coordinated with your export compliance officer for any export control issues and/or Technology Control Plans or updates?
- ☐ Have you used screening tools- i.e., DOC ITA Consolidated Screening- to ensure that foreign organizations are compliant with U.S. laws and regulations?
- ☐ Maintain awareness of competitor nation interest in your research space.
- ☐ Do you have any item, software, technology, project, etc. requiring protection per the EAR or ITAR?

Appendix E. Technology Control Plan (TCP) Template

Technology Control Plan

Project Title:

Organizational Unit:

Responsible Individual: *First and last name, division name and number, extension, and email. Also list an alternate to serve as backup in the absence of the principal.*

Scope of Activities or Locations: *For project-based TCPs, list work activities covered by this TCP. Work may be described in the form of projects or other units of activity that make up the portfolio of OU activities. For location-based TCPs, list all the locations covered by this TCP.*

Effective Date: *Month, Day, Year (e.g., October 1, 2017)*

Source of Funding: *List source(s) of funding for work activities or locations covered by this TCP (e.g., organizational, and other sources).*

Applicable Agreements: *List applicable agreements for work activities or locations covered by this TCP. List any restrictions required in these agreements.*

Technical Description: *Provide technical description of "export controlled" items, technologies, and activities. Provide applicable export control jurisdiction, classification, and controls (protections, license requirements, and exceptions/exemptions) for the items, technologies, and activities/locations covered by the TCP.*

Physical Security Plan: *Describe plan to physically secure and shield spaces and areas containing controlled items, technologies, and activities from unauthorized/unintentional "release of technology, software, or technical data" (See* Definitions*) to foreign persons.*

- ***Location:*** *Identify the physical location(s) (Building/Room Number) for each controlled item, technology, and activity. A schematic of the immediate location is recommended.*
- ***Security Measures:*** *Describe security measures to protect each technology, software, or technical data from unauthorized/unintentional release (e.g., locked doors, electronic access controls, security badges, limited access).*
- ***Perimeter Security:*** *Describe perimeter security features of the location(s) containing controlled items, technologies, and activities.*

Information Security Plan: *Describe plan to secure computers, networks, electronic transmissions, and databases containing information associated with controlled items, technologies, and activities from unauthorized/unintentional release to foreign persons. Work with your IT Security Officer to ensure the following components—as well as related physical security and item security components—are addressed in the respective System Security Plan (SSP), and thus reference the SSP herein.*

- ***System Setup:*** *Describe the setup of the information technology system(s) that will contain information associated with controlled items, technologies, and activities. A schematic of the system setup is recommended.*
- ***Security Measures:*** *Describe security measures to protect information associated with the controlled items, technologies, and activities (e.g., password access, firewall protection, encryption, and secure network communications to/from authorized persons).*

- ***Access Management:*** *Describe how release of information associated with controlled items, technologies, and activities will be restricted only to authorized foreign persons and discontinued when the individuals are no longer authorized (e.g., employee or associate no longer working on the activities—or in spaces—covered by this TCP).*

- ***Restricted Communications:*** *Describe plan to protect export-controlled information during conversations. How will discussions about controlled items, technologies, and activities be limited to authorized foreign persons and only areas/spaces where unauthorized foreign persons are not present. How will discussions with third parties occur (e.g., under agreements that respect limitations on foreign person disclosures).*

Item Security Plan: *Describe plan to secure tangible items to safeguard against unauthorized/unintentional release of technology, software, or technical data to foreign persons.*

- ***Item Marking:*** *Describe measures to clearly identify and mark tangible items that are export controlled or contain export-controlled information*.

- ***Item Storage:*** *Describe physical security measures to store—and prevent unauthorized access to: (a) soft and hardcopy data, lab notebooks, reports, and other materials containing export-controlled information; and (b) equipment, internal components, associated operating manuals, and schematic diagrams that are export controlled or contain export-controlled information (e.g., locked storage, key/electronic controls).*

Training Plan: *Describe any special export control training required for the activities and spaces covered by this TCP.*

Recordkeeping Requirements: *Describe any special or non-standard project-specific security measures for retention/disposal of items or technologies.*

Approval Signatures:

Certification: I hereby certify that I have read and understand this TCP and my obligations under federal export control laws and regulations and NIST export controls management policy and associated directives regarding the items, technologies, and/or activities identified in this TCP. I agree to take the actions set forth in this TCP and, if applicable, to comply with the terms of any license governing the items, technologies, and/or activities and the terms in any applicable agreements regarding such items, technologies, and/or or activities. I also agree to maintain a list of foreign persons to whom "release of technology, software, or technical data" covered by the TCP is authorized or not authorized. Each authorized U.S. and foreign person shall be informed of the conditions of the TCP and agree to comply with the security measures described in the TCP before covered technology, software, or technical data is released.

Principal Investigator:

Print Name	Signature	Date

Supervisor:

Print Name	Signature	Date

Export Control Officer:

Print Name	Signature	Date

[The signed and approved TCP shall be maintained by the Principal Investigator. A copy of the TCP shall be filed with the Export Control Officer of the Safeguarding International Science Research Security Team. If one or more foreign associates will be working on the activities covered by this TCP, the TCP shall be included as part of the nomination/approval process for each of the foreign national associate.