NIST IR 8484 Research Security Plan Guidance & Template

Introduction

The United Sates (U.S.) retains its science and technology (S&T) leadership by actively engaging with the international research community in areas of mutual interest and benefit. This includes welcoming international scientists into U.S. research laboratories (e.g., Federal, academia, and industry) to collaboratively perform cutting-edge joint-research. Coupled with that, the national and economic security of the U.S. depends on effective risk management practices for organizations that engage in international research collaborations.

The first step in implementing a Research Security Program (hereinafter referred to as "Program") is the development of a research security plan (hereinafter referred to as "plan") to meet the requirements of Federal funding initiatives. A well-developed plan creates the foundation and path forward to a risk-balanced Program that safeguards the research ecosystem. Using the NIST IR 8484, "Safeguarding International Science Research Security Framework" as a baseline to create a plan, enables an organization to ultimately implement a program that mitigates research security risks while enhancing the benefits of collaborating with the best talent available. The Framework's methodology is designed to protect individual privacy and civil liberties while assessing potential risks of engagement; and to assist organizations, regardless of size, risk profile, or contribution, in applying the principles and best practices of a balanced, risk management effort.

A template is included at Appendix A of this document to further simplify plan development. The NIST Research Security Team is readily available to assist an organization in the development of a Plan. Requests may be sent to researchsecurity@nist.gov.

What is safeguarding science and research security? This a common question when starting to develop a plan.

> Safeguarding science facilitates open science and research that values international collaboration while protecting U.S. national security and economic security interests.
>
> Research security is a risk management methodology designed to protect the means, know-how, products, and results of research until they are ready to be shared.

A well-developed plan contains three objectives:

- Maintain an inclusive culture that promotes international collaborative science while safeguarding the U.S. research enterprise.
- Develop and implement a strategic communication plan inclusive of leadership, management and principal investigators.
- 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.

The basic components of a plan are discussed below and incorporated into the template found in Appendix A of this document.

Components

Using the Framework's Key Elements and Characteristics (Section 4.3) as a starting point, a plan includes:

Organizational leadership

The plan shall identify the organization's leadership.

Organizational Policy

The plan shall identify the organizational policy that establishes requirements for an integrated, mission-focused, risk-based approach for international science and technology collaborations that provide safeguards against undue foreign interference while protecting the openness and integrity of the research ecosystem.

Scope of Program

The policy shall identify the scope of the program. As a minimum, the plan shall identify what types of reviews shall be incorporated into the program. As shown in NIST IR 8484 Section 7, this includes:

- Research associate appointments
- Foreign travel
- Foreign collaborations and publications
- Funding to external organizations

Research security team

The research security plan shall identify team members, a team lead, and their roles and responsibilities.

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. A team lead must be codified at the beginning.

Part of the team development is recognizing available resources within an organization that may be integrated as either team members or *ad hoc* to prevent duplicative efforts.

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, and
- Cybersecurity.

Technology and intellectual property assessment

The plan must contain a minimum list of technologies and intellectual property (e.g., critical asset list) that are pertinent to a funding application that are at risk from foreign adversaries seeking to gain an advantage. This includes research that is fundamental and proprietary.

The plan must contain acknowledgment that the research security team will use of National Security Presidential Memorandum 28 (NSPM-28) Operations Security (OPSEC) to perform an in-depth technology risk assessment.

Communication and training

The plan shall cover a communication and training strategy to educate staff and explain the importance of how a program safeguards international science. An example of strategic components is found in NIST IR 8484 Section 6 – Communication and Integration and may be used by the applicant to develop a list of proposed elements.

Technology Control Plans

The plan shall define an organization's technology control plan (TCP) that incorporates export control, cybersecurity, and data management. A TCP integrates the OPSEC technology risk assessment outcomes. The organization shall identify a TCP for each application. A TCP template is found in NIST IR 8484 – Appendix E and may be identified in the plan as part of an organization's research security program implantation.

Reviews, Risk Determination, and Mitigation

The plan shall identify a research security review methodology. NIST IR 8484 – Section 7 covers best practices guidance for mission-focused review methodologies; Section 8 covers risk-balance determination and mitigation strategies. These sections may be identified in the plan as part of an organization's research security program implantation.

Acceptance and Implementation

The plan shall identify an acceptance of an implemented program through the Research Security Team. Additionally, the plan shall outline a proposed program implementation timeline for the organization.

Appendix A: Research Security Plan Template

(Insert Organization Name) Research Security Plan

Organizational leadership

Identify the organization's leadership.

- Name of organization
- Names and positions of organization's leadership
- Point of contact

Organizational Policy

Attach the existing research security policy or the intent to develop such policy. For an organization needing to create a research security policy, please provide a timeline.

Scope of Program

Provide the research security scope or the intent to develop such scope. For an organization needing to create a research security scope, please provide a timeline.

Research security team

Provide the research security team membership.

- Name, position, and e-mail contact
- Roles and responsibilities of team members

For an organization needing to create a research security team, please provide a timeline.

Technology and intellectual property assessment

Attach an existing critical asset list that contains a minimum list of technologies and intellectual property that are pertinent to a funding application that are at risk from foreign adversaries.

For an organization needing to create a critical asset list, please provide a timeline.

Communication and training

Describe the current communication and training strategy. Please include type of training provided.

For an organization needing to create a communication and training strategy, please provide proposed communication strategy, a proposed training scope, and a timeline.

Technology Control Plans

For an organization with existing TCPs, please attach.

For an organization without an existing TCP, please identify the intended solution and timeline.

Reviews, Risk Determination, and Mitigation

Identify a research security review methodology and provide a timeline.

Acceptance and Implementation

Outline a proposed research security program implementation timeline for the organization.