Analysis of NIST Safeguarding International Science Research Security Framework

In August 2023, the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) issued a new report entitled Safeguarding International Science Research Security Framework ("Framework"). The Framework provides a lengthy and detailed description of a possible structure for an institutional research security program (RSP) that addresses the requirements of Presidential Memorandum 33 on United States Government-Supported Research and Development National Security Policy ("NSPM-33"), including review processes for five different categories of international collaborative activities and associated checklists and tools. Use of the Framework is *not* mandatory, but NIST encourages institutions to scale and adapt the Framework to meet their specific circumstances and requirements. To assist academic research institutions in evaluating implementation of the Framework, this document provides an overview of the Framework's major components and concludes with an assessment of difficulties institutions may encounter in implementing the Framework in an academic research setting.

Purpose of the Framework: NIST developed the Framework to assist government agencies, academia, and industry in addressing the requirements of NSPM-33 and several other U.S. government research security policy documents.[1] The Framework establishes a set of "recommended security best practices" and a methodology for implementing an institutional RSP. These practices cover a range of activities that involve international engagement including foreign appointments, foreign travel, foreign collaborations, foreign funding, and provision of products/services to foreign entities. NIST describes the Framework's design as being "holistic, scalable, and adaptable to meet the different mission needs of the science and research community" and notes that the Framework is distinct from but complementary to the NIST Cybersecurity Framework.

Implementation Requirements: The chart on the next page outlines the Framework's overarching RSP implementation requirements. NIST stresses that an institution's RSP should aim to promote international collaboration while protecting research from "undue foreign threats or influence," including potential theft of intellectual property, trade secrets, and proprietary information.

[1] These documents include the JCORE Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise, National Security Presidential Memorandum 28 Operations Security (NSPM-28), and the Office of the Director of National Intelligence (ODNI) Safeguarding Science Toolkit.

Overarching Requirement	Implementation Details
Assessment & Analysis	• Conduct an organizational assessment to identify critical assets, potential foreign threats, and areas of vulnerability. • Analyze current business processes under the lens of current research security guidance and develop appropriate risk mitigation countermeasures.
Protocols	• Develop research security protocols to "safeguard international science initiatives," leveraging existing business processes when possible.
Reviews	• Conduct risk-based reviews of international science programs and activities and use the results of these reviews to inform which activities should take place and appropriate mitigation measures.
Training & Guidance	• Develop guidance/methods to safeguard international collaborations including discussion of current threats/vulnerabilities. • Provide organizational research security awareness training and tools/resources for "standard application across the organization."
Communications	• Provide forums for discussing/evaluating threats and security practices.
Partnerships	• Develop partnerships across internal units that play a role in research security (e.g., IT, HR, etc.) and partner with external organizations (e.g., government agencies, partner organizations, etc.) to identify and address research security issues.

RSP Implementation: In developing their RSPs, NIST emphasizes the need for institutions to have:

Transparent Methodologies

- Communicate to staff why the RSP is important
- Adopt methods to promote understanding of the RSP and its' implementation

Clear & Defensible Policies and Processes that:

- Are "mission focused, non-invasive, and non-intrusive"
- Clearly define the RSP, and its organization and oversight
- Ensure the RSP can withstand outside audit

Key RSP Elements

- Multi-disciplinary research security team
- Organizational communication and integration plan
- Review processes for international activities
- Risk-balanced methodology for determining which international activities to undertake and how to handle them
- Export control and technology control plans and compliance procedures

Research Security Team: The NIST Framework includes recommendations for structuring a team of institutional personnel that will lead efforts in developing and implementing the RSP. The chart below lists the Framework's recommended team members, along with their qualifications and duties.

Team Member	Qualifications	Responsibilities
Research Security Team Lead	Technical, scientific, and research expertise for performing assessments of foreign collaborations and making risk management determinations.	• Leads discussions on RSP set-up, protocols, training, etc. • Leads collaborative efforts among inter-institutional units and with outside agencies/groups. • Makes risk mgmt. determinations based on information received from team.
International Affairs Mgr.	International program and foreign affairs expertise for assessment of international agreements, benefits of specific foreign collaborations, and international science and policy considerations.	• Assesses international academic exchange and other agreements. • Considers risk/benefit of proposed international collaborations/activities. • Evaluates science and technology policy implications of activities as part of risk analysis.
Export Control Mgr.	Expertise in U.S. export control/trade regulation laws/regulations.	• Evaluates and determines export control licensing and disclosure obligations associated with transfer of technology, data, commodities, software, etc. associated with proposed foreign collaborations/activities.
Information Security Officer	Expertise in information technology security requirements, system vulnerabilities, and IT threat arena, as well as in system structures, tools, mechanisms, etc. to promote/foster IT security.	• Evaluates system access, vulnerabilities, and overall system integrity and impacts of proposed foreign collaborations/activities on IT systems/security.
Research Security Officer	Security, intelligence, counterintelligence, and risk management expertise.	• Evaluates research security/inappropriate collection of information and threats associated with proposed foreign collaborations/activities.
Ad Hoc Team Members	As needed, the research security team will include representatives from legal counsel, school/departmental/programmatic leadership, physical plant security, office of sponsored programs, technology transfer, compliance office, etc.	

Team Reporting: The Framework advocates a hierarchical structure of reporting to institutional leadership. Bi-weekly reporting to upper-level administration is recommended.

Team Meeting Structure: NIST recommends that research security team members meet every two weeks. As necessary, the team should establish and convene subcommittees and working groups (chaired by a member of the research security team).

Communications and Integration: NIST also emphasizes the need for solid lines of communications regarding the RSP, along with efforts to integrate the RSP into the institutional culture, including:

- Implementing institution-wide communications concerning the RSP (e.g., newsletters, town halls, email blasts).
- Establishing a central website, central email, and regular "open-office hours" for the Research Security Team.
- Engaging key institutional staff who will advocate for the RSP.
- Ensuring top level managerial support for the RSP, including buy-in to program's value and provision of appropriate RSP funding/resources.
- Requiring initial and recurrent periodic training on organizational requirements (e.g., foreign travel, cybersecurity, physical security) for all staff who support activities covered by the RSP. The RSP also should include, at a minimum, annual training on staff responsibilities and changes in threat environment; as well as program and/or activity-specific training.
- Documenting policies and processes and ensuring they are easily accessible and shared across the institution.

Institutional Reviews of International Activities: The bulk of the Framework consists of **very detailed** processes that institutions can adapt and employ for the review of specific activities in each of the five following categories: (i) research associate appointments; (ii) foreign travel requests; (iii) foreign collaborations; (iv) foreign requests for products/services/software tools; and (v) extramural funding opportunities.

Each of the five review processes includes the following items:

- Description of scope of activities to be reviewed.
- Type and sources of information (e.g., CV, social media, researcher disclosures, information associated with persistent digital identifiers) to be collected for review.
- Key questions to ask, and, in some cases, directions as to whether in-person interviews should be conducted.
- Lists of resources and tools (e.g., screening lists, regulations, social media, databases, standards) that may be used to vet collected information.
- Common indicators/warnings of the risk of undue foreign influence (e.g., financial ties to organization in country of concern, participation in foreign talents programs, requests to access research projects unrelated to area of research).
- Potential countermeasures/risk mitigation tools.
- Diagram of the review process indicating roles and responsibilities and possible outcomes
- Review forms for documenting answers to key questions, collection of key information, potential risks and benefit to organization, risk mitigation devices (e.g., technology control plan), risk level determination, review process, and review decision. [NOTE: No review form is provided for the "foreign collaborations" category.].

- Checklist of considerations to weigh in performing a risk/benefit analysis of the information collected for the review.

The chart on the next page provides the following information for each review category described in the Framework: potential scope of the assessment, brief summary of key issues/information to consider, and a sample of identified risk indicators. Notably, the Framework advocates the use of the screening lists/tools in reviewing collected information including: Australia Strategic Policy Institute China Defense University Tracker ("ASPI Tracker"), International Trade Administration Consolidated Screening Lists (ITA CSL), Critical Emerging Technology List, and Export Administration Regulation (EAR) and International Traffic in Arms Regulations (ITAR) lists. The chart collectively refers to these lists/tools as "Screening Lists."

Risk Factor Review and "Risk Balanced" Determinations Regarding International Collaborations / Activities: The Framework contemplates that in reviewing the activities in each of the five categories, the research security team will analyze the information collected to identify and understand the risks posed, and then balance these risks against the potential benefit to the organization to determine if/how to proceed with respect to an activity, along with determination as to what, if any, countermeasures should be implemented to mitigate risk.

Identification and Understanding of Associated Risks: The Framework identifies the following 15 risk components for consideration in evaluating threats to "national security, national economic security, or intellectual property security":

Non-Traditional Information Collectors	Critical and Emerging Technologies	Technology Gaps	Conflicts of Interest	Conflicts of Commitment
Cybersecurity Risks	Physical Access	Insider Threats	External Organizations	External Funding
Patterns of Concern	Intellectual Property	NIST Cybersecurity Program Suite	NSPM-28 Operations Security Program	User Activity Monitoring

The Framework discusses for review of some risks that academic institutions have experience in assessing, (e.g., potential theft of intellectual property, conflicts of interest, and conflicts of commitment). However, it also calls for review and understanding of broader risks to U.S. national security and military interest that are difficult to assess (e.g., Whether "transfer of fundamental research" may be compiled "to accelerate foreign military applications" or "accelerate foreign civil applications"?, Whether research on critical and emerging technologies involves potential "military-civil fusion technology applications" or a potential solution to fill a foreign country's "technology gap"?)

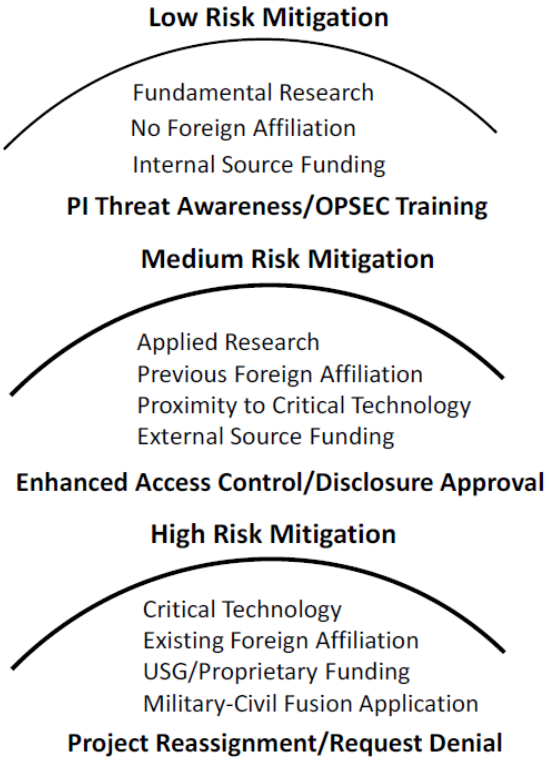
COGR

Overview of Framework Review Processes

Category	Potential Scope of Review	Summary of Key Issues & Information Sources to Evaluate	Sample of Key Risk Indicators
Research Associate Appointments	• Foreign national associates (non-U.S. citizens or permanent residents) as potential "insider threats" and vectors of undue foreign influence (e.g., participation in foreign talents program). • Non-institutional employee domestic associates who are U.S. citizens/permanent resident as potential "insider threat. • (NOTE: Screening of domestic associates is outside the scope of NSPM-33.)	• Affiliations and origin and method of recruitment • Legal status (e.g., visa) • Funding source • Host/sponsor affiliations • Project details (e.g., type of research, any export-controlled technology, technology type, and applications, patent potential) • Sample Info Sources: CV, internet, social media, Screening Lists, and persistent digital identifiers (PDIs)	• Association with entity on ASPI Tracker • Association with a Chinese Seven Sons of National Defense institute • Foreign talent or malign foreign talent recruitment program (FTP/MFTP) participation • Foreign funding/scholarship from Country of Concern (COC) (e.g., Chinese Scholarship Council funding)
Foreign Travel Requests	• Virtual and in-person foreign meetings and visits for potential inappropriate transfer of intellectual property/capital and undue foreign influence. • In-kind assistance from foreign sources or reimbursement for expenses for potential conflict of interest/commitment and undue foreign influence. • (NOTE: Framework includes review of virtual travel, which is outside the scope of NSPM-33.)	• Purpose of travel, event type, reason for attendance • Type of travel – physical or virtual • Host organization for event • Location of travel • Foreign funding or assistance in kind (AIK) to support travel • Research funding source • Type of research (e.g., export controlled, technology type, and applications) • Sample Info. Sources: Travel request form, invitation, offer of AIK/reimbursement, internet, Screening Lists, and event website	• Invitation and/or support/AIK from organization in/affiliated with COC • Reason for attendance tied to critical emerging technology • Event located in/sponsored by COC/COC affiliated organization or organization affiliated with MFTP • Lack of information about event, sponsor, purpose • Private "invitation only" event associated with COC • Event involves emerging technologies, on which a competitor nation's researchers are seeking to collaborate
Foreign Collaborations	• Evaluation of collaboration at initiation and when a publication is ready for submission to a journal for potential conflict of interest/commitment, theft/inappropriate transfer of intellectual property, and undue foreign influence (e.g., FTP/MFTP).	• Participants and their organizations and funding sources • Type of research (e.g., export controlled, technology type, and applications) and patent potential • Research funding source • Sample Info. Sources: CV, internet, screening lists, institutional scientific experts, and PDIs. • (NOTE: Framework suggests pre-publication review if authors are from COCs and disallowance of publication if authors have ties to MFTPs.)	• Collaborator is citizen of COC, associated with MFTP, or high-risk military-civil organization • Research involves critical emerging technology that is the focus of a COC • Research is not expected to be published or is associated with product/service engagement • Collaborators have funding from COC or MFTP

Category	Potential Scope of Review	Summary of Key Issues & Information Sources to Evaluate	Sample of Key Risk Indicators
Foreign Request for Products, Services, Software	• Products/services produced and sold and/or access to databases/online research tools will provide access to potential military-civil fusion technology. • Compliance with export controls.	• Type of product/service to be provided and type of technology it involves (e.g., export controlled, technology type, and applications) • Requesting foreign organization • Sample Info Sources: Technical experts, internet, Screening Lists	• Product/service requested by COC-affiliated organization includes dual-use/critical emerging technology • Researcher has current/past affiliations with COC • Requests for source code • Request for same product from multiple COC organizations • Request for large quantities of product/service
Extramural Funding Opportunities	• Identification of conflicts of interest and conflicts of commitment. • Review for compliance with the provisions of Division A of the CHIPS & Science Act's regarding receipt and use of incentives received under the Act. • Fulfillment of SBIR and STTR due diligence disclosure requirements under SBIR and STTR Extension Act of 2022. • (NOTE: Review of compliance with CHIPS & Science Act incentive requirements is outside the scope of NSPM-33.)	• Funding organization • Person seeking funding and their affiliations and research funding sources • Type of technology being researched (e.g., export controlled, technology type, and applications) • Potential patents • Financial structure and ties of funding organization (e.g., ownership, subsidiaries, affiliations, obligations) • Sample Info Sources: CV, internet, current and pending support/biosketch disclosures, third-party analytics, Screening Lists, PDIs, social media, and contractual agreements	• The foreign funding source is an organization affiliated with a COC • Funding involves research regarding technology in which a COC has an interest • Researcher has current/past affiliations with COC research institution or FTP • Funding organization has disclosed or undisclosed financial ties to COC-affiliated organization

Determination Process: The Framework suggests that research security team members and any other required institutional representatives hold review meetings to review the risk and benefit factors associated with an activity, vote to assign a risk mitigation level and any required risk mitigation measures (e.g., specific training, external funding agency approval of foreign participation, limited project access, risk assessment or research workspace, etc.), and determine whether or not to concur with the conduct of the international activity. The Framework includes the following risk stratification construct:



Additionally, if a project involves export-controlled information/technology, institutions need to adhere to export control review processes and use of appropriate technology control plans, a template for which in included in the appendices to the Framework.

Review Process Documentation: The Framework suggests that results of all risk determination reviews should be electronically maintained in a controlled-access network site that is secured from unauthorized access. Government agencies employing the framework must also determine whether records warrant designation as Controlled Unclassified Information (CUI).

Conclusion: Implementing the Framework in Academic Research Environment

The Framework provides many sample tools, forms, and processes that institutions will find helpful as they develop their research security programs, but some features of the Framework (e.g., detailed consideration of national security impacts) are geared toward government agencies and the knowledge base/perspective that those agencies possess. For example, many institutions will simply not have the expertise to evaluate whether certain fundamental research may impact "gap technologies" that are critical to the economic or military advancement of a competitor nation. Thus, implementation of the Framework as a whole, without significant tailoring, is likely unfeasible for many universities. Fortunately, the Framework acknowledges that it is not a one-size-fits-all document and may be adapted and scaled to different settings.

On a more fundamental level, however, academic institutions may have difficulties in integrating the Framework's detailed review processes into their cultures. First, academic institutions are notoriously decentralized, information is often siloed, and faculty members typically act independently with respect to their research activities. The Framework, however, contemplates a highly centralized review process in which a hierarchically organized research security team has significant access to information about researcher activities and the authority to review and make decisions regarding these activities.

Second, academic institutions are grounded in principles of academic freedom, particularly regarding collaborations and publications in the fundamental research space. In this environment, broad institutional review of collaborations and features such as "pre-publication" review for assessment of co-authors' affiliations/funding may run headlong into institutional policies/principles concerning academic freedom (and in the case of publication restrictions, fundamental research requirements). Although research institutions recognize the need to abide by funding agency requirements, it must be noted that the Framework does not explicitly tie review activities to only federally funded projects or to compliance with federal agencies' requirements. Indeed, given the breadth of activities that NIST suggests be reviewed and the extremely detailed nature of the review processes, it becomes difficult to see how these processes could ever meet the Framework's stated goals that they be "non-intrusive" and "non-invasive."

Finally, the cost and associated administrative burden of implementing the Framework's detailed and wide-ranging review processes in a university setting would be substantial. Many institutions do not have the resources to hire new staff devoted solely to research security and will allocate research security responsibilities to existing employees to perform in addition to their current job duties. This will be particularly true in emerging research institutions and other institutions that do not have mature compliance structures. Moreover, even in the case of fundamental research, which the Framework identifies as "low risk" under its risk mitigation construct, the Framework does not incorporate the use of risk analysis to determine *which activities require review in the first place*. Rather, the document contemplates the collection of significant amounts of information and detailed review of **all** foreign collaborative activities to determine where they fall on the risk spectrum. Such an approach does not take into consideration institutional resource constraints and the need to ensure that scarce resources are first allocated to activities that present the greatest degree of risk.