NSF SECURE Center

RESEARCH SECURITY

RISK ASSESSMENT FRAMEWORK

NSF SECURE Center

RESEARCH SECURITY
RISK ASSESSMENT FRAMEWORK

INTRODUCTION

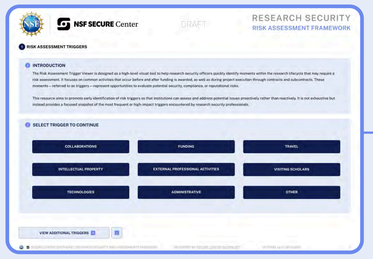
This guided research risk assessment tool is designed to support research security officers and compliance professionals in conducting consistent, thorough, and well-informed risk assessments. Developed through the NSF SECURE Center, the materials reflect common scenarios and regulatory expectations encountered across institutions of varying sizes and capabilities.

The package includes four interlinked resources:

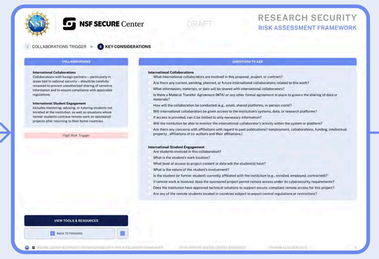
1. Trigger Viewer – Identifies research activities that may prompt a risk review.
2. Risk Assessment Key Considerations – Provides guiding questions to deepen understanding of flagged activities.
3. Tools and Resources – Offers vetted free and paid tools to support investigation and documentation.
4. Risk Assessment Summary Template – Assists in summarizing and archiving findings for institutional records and compliance.

These resources were built by and for research security professionals to encourage shared understanding, improve response consistency, and prepare for sponsor inquiries or audits.

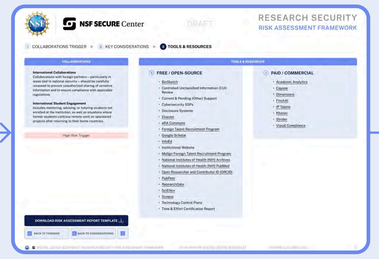
HOW TO USE



1 Select a Trigger



2 Review Key Considerations



3 Use Tools & Resources

4 Fill Risk Assessment Summary Template

TARGET AUDIENCE

- Research Security Officer
- Principal Investigator
- Research Administration Support Offices

PURPOSE & BENEFITS

Establishes a Common Starting Point
Outlines triggers for when a risk assessment should begin.

Promotes Consistent Evaluation
Offers structured questions to uncover relevant facts, reducing guesswork.

Enables Actionable Research
Connects activities to tools that support fact-finding, validation, and due diligence.

Supports Compliance and Recordkeeping
The included summary template ensures documentation is retained and accessible.

Future-Ready Design
This framework is a foundation for future digital tools that will streamline workflows through guided, interactive pathways.

CLICK HERE TO CONTINUE

1 RISK ASSESSMENT TRIGGERS

INTRODUCTION

The Risk Assessment Trigger Viewer is designed as a high-level visual tool to help research security officers quickly identify moments within the research lifecycle that may require a risk assessment. It focuses on common activities that occur before and after funding is awarded, as well as during project execution through contracts and subcontracts. These moments — referred to as triggers — represent opportunities to evaluate potential security, compliance, or reputational risks.

This resource aims to promote early identification of risk triggers so that institutions can assess and address potential issues proactively rather than reactively. It is not exhaustive but instead provides a focused snapshot of the most frequent or high-impact triggers encountered by research security professionals.

HOW TO USE

- Start by reviewing the categorized list of risk triggers, organized by High, Medium, and Low risk levels. These groupings help prioritize attention based on the likelihood and impact of potential research security concerns.
- Clicking on any trigger will take you to a detailed view, where you'll find a short description of the activity and a curated list of key considerations — questions designed to guide your preliminary risk assessment and uncover important context.
- This tool is intended to help research security officers quickly identify and begin evaluating research activities that may warrant deeper review, serving as the entry point for the full risk assessment process.

TARGET AUDIENCE

- Research Security Officer
- Principal Investigator
- Research Administration Support Offices

PURPOSE & BENEFITS

Proactive Risk Management
Identifies common high-risk activities reducing risk of compliance or regulatory issues.

Structured Approach
Connects activities to a defined point in the research lifecycle for clarity and planning.

Shared Language
Supports internal alignment across teams by offering a common vocabulary for risk triggers.

Scalable
Can be used across institutions of various sizes and adapted as needed.

VIEW RISK ASSESSMENT TRIGGERS →

1 RISK ASSESSMENT TRIGGERS

INTRODUCTION

The Risk Assessment Trigger Viewer is designed as a high-level visual tool to help research security officers quickly identify moments within the research lifecycle that may require a risk assessment. It focuses on common activities that occur before and after funding is awarded, as well as during project execution through contracts and subcontracts. These moments — referred to as triggers — represent opportunities to evaluate potential security, compliance, or reputational risks.

This resource aims to promote early identification of risk triggers so that institutions can assess and address potential issues proactively rather than reactively. It is not exhaustive but instead provides a focused snapshot of the most frequent or high-impact triggers encountered by research security professionals.

SELECT TRIGGER TO CONTINUE

COLLABORATIONS | FUNDING | TRAVEL

INTELLECTUAL PROPERTY | EXTERNAL PROFESSIONAL ACTIVITIES | VISITING SCHOLARS

TECHNOLOGIES | ADMINISTRATIVE | OTHER

DISCLAIMER

- This list of triggers may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use of this list is at your own discretion, and always review any data or content before relying on it.

VIEW ADDITIONAL TRIGGERS

2 RISK ASSESSMENT KEY CONSIDERATIONS

INTRODUCTION

The Risk Assessment Key Considerations resource builds upon the first step — the Trigger — by offering structured, probing questions aligned to specific research activities that have been identified as risk triggers.

Once a trigger has been identified, the Key Considerations resource helps research security officers explore the underlying risk factors in greater depth. This section presents tailored questions and prompts to uncover potential concerns across various domains — such as collaborations, funding, or travel.

The goal is to guide a thoughtful and structured review of each activity, ensuring that all relevant details are surfaced. While not every question will apply in every case, this tool supports comprehensive and consistent assessments.

HOW TO USE

- After identifying a trigger, use this section to guide your deeper review. It offers structured questions tailored to each research activity — such as funding, collaborations, or visiting scholars — to help uncover relevant details and risks.
- You don't need to answer every question. Instead, use them to focus your assessment, find information gaps, and decide if further review is needed. This builds on the Trigger Viewer by helping you move from identifying an issue to understanding it.
- Not all questions may apply in every situation — but they are listed to ensure completeness and consistency in risk evaluation. This list may not be comprehensive and additional considerations may need to be assessed dependent upon the specific situation.

TARGET AUDIENCE

- Research Security Officer
- Principal Investigator
- Research Administration Support Offices

PURPOSE & BENEFITS

Contextual Depth
Helps RSOs explore the nuance of each trigger to identify potential regulatory, security, or reputational concerns.

Guided Review
Serves as a reference for staff members and ensures standardization across reviewers.

Flexible Utility
Can be used in intake interviews, internal reviews, or documentation gathering.

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

CONTINUE TO KEY CONSIDERATIONS

COLLABORATIONS	QUESTIONS TO ASK
International Collaborations Collaborations with foreign partners — particularly in areas tied to national security — should be carefully reviewed to prevent unauthorized sharing of sensitive information and to ensure compliance with applicable regulations.	**International Collaborations** ☐ What international collaborators are involved in this proposal, project, or contract? ☐ Are there any current, pending, planned, or future international collaborations related to this work? ☐ What information, materials, or data will be shared with international collaborators? ☐ Is there a Material Transfer Agreement (MTA) or any other formal agreement in place to govern the sharing of data or materials? ☐ How will the collaboration be conducted (e.g., email, shared platforms, in-person visits)? ☐ Will international collaborators be given access to the institution's systems, data, or research platforms? ☐ If access is provided, can it be limited to only necessary information? ☐ Will the institution be able to monitor the international collaborator's activity within the system or platform? ☐ Are there any concerns with affiliations with regard to past publications? (employment, collaborations, funding, intellectual property , affiliations of co-authors and their affiliations.)
International Student Engagement Includes mentoring, advising, or tutoring students not enrolled at the institution, as well as situations where former students continue remote work on sponsored projects after returning to their home countries.	**International Student Engagement** ☐ Are students involved in this collaboration? ☐ What is the student's work location? ☐ What level of access to project content or data will the student(s) have? ☐ What is the nature of the student's involvement? ☐ Is the student (or former student) currently affiliated with the institution (e.g., enrolled, employed, contracted)? ☐ If remote work is involved, does the sponsored project permit remote access under its cybersecurity requirements? ☐ Does the institution have approved technical solutions to support secure, compliant remote access for this project? ☐ Are any of the remote students located in countries subject to export control regulations or restrictions?
High Risk Trigger	

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

NSF SECURE Center

RESEARCH SECURITY
RISK ASSESSMENT FRAMEWORK

1 FUNDING TRIGGER ▶ 2 **KEY CONSIDERATIONS**

FUNDING

Federal Funding
Research projects funded by U.S. government agencies may require a research security review.

Commercial Research Funding
Sponsored research supported by non-federal sources, such as commercial entities or non-profit research organizations.

International Sponsors / Foreign Source of Support
Research sponsored by organizations or entities based outside the United States.

Grant Funding with Restrictions
May include limitations on publishing, personnel eligibility, commercial NDAs, export controls, CUI involvement, or CMMC compliance requirements.

High Risk Trigger

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

QUESTIONS TO ASK

Federal Funding

- [ ] What current federal funding do the investigators have?
- [ ] What past federal funding have the investigators received? (Specify agencies such as DoD, DOE, NSF, etc., and note if any of the funding was restricted.)
- [ ] Does the investigator's disclosure capture the new requirements related to MFGTRP (Manufacturing and Foreign Talent Recruitment Program)?
- [ ] Are investigators receiving any training related to Research Security (RS), MFGTRP compliance, or foreign travel requirements?
- [ ] Is the Research Security Office prepared to provide ad hoc training to investigators if a risk review identifies the need?
- [ ] Is there a process during pre-award or post-award review to identify research security requirements tied to specific awards?
- [ ] Are awards administrators trained or informed about what research security red flags to look for and when to involve the Research Security Office in the review process?

Commercial Research Funding

- [ ] Do the investigators have any non-federal funding sources?
- [ ] What non-federal funding sources are currently supporting the investigators' work? (Please specify commercial entities, foundations, non-profits, etc.)
- [ ] If investigators also have federal funding, has all non-federal support been properly disclosed to the relevant federal agencies?
- [ ] Have any intellectual property (IP) agreements or relationships with commercial partners been reviewed by the institution's Tech Transfer Office or legal counsel?
- [ ] Does the commercial entity require access to the institution's IT infrastructure?
- [ ] If so, does the IT infrastructure contain or co-mingle with government data or federal covered systems?
- [ ] Can the institution segment or otherwise limit the commercial entity's access to sensitive or federally controlled information?
- [ ] Does the commercial entity require physical access to any facilities that support federal research activities?
- [ ] If so, can physical access be managed to limit exposure to federally controlled information or research activities?

International Sponsors / Foreign Source of Support

- [ ] Do the investigators have any foreign sources of funding?
- [ ] If yes, please provide details about the foreign funding sources (e.g., country, organization, nature of the support).
- [ ] Have investigators received any gifts, support, or promises of future support from foreign entities?
- [ ] Are investigators aware of how support, gifts, or future promises could relate to Foreign Talent Recruitment Programs (FTRP)?
- [ ] Has appropriate training been provided to investigators to ensure they understand the definitions and disclosure requirements related to foreign support and FTRP?

Grant Funding with Restrictions

- [ ] Are there any restrictions associated with the investigator's current funding awards?
- [ ] Are any of the awards contracts rather than grants (since contracts typically impose more restrictions)?
- [ ] Has Export Control reviewed the awards for potential restrictions such as cybersecurity requirements (e.g., CUI or CMMC compliance), publication restrictions, limitations on foreign national participation, or other compliance needs?
- [ ] For Controlled Unclassified Information (CUI), is the intended IT environment compliant with CUI requirements?
- [ ] Is there an SPRS (Supplier Performance Risk System) score available for the institution's enterprise or the specific project enclave?
- [ ] Does the institution have a CUI-compliant delivery method (e.g., Microsoft GCC High), especially considering that standard email systems do not meet NIST 800-171 compliance?
- [ ] Is there a CUI-compliant virtual meeting solution (such as Zoom for Government or Microsoft Teams GCC High) available for project communications?

VIEW TOOLS & RESOURCES

1 TRAVEL TRIGGER ▶ 2 **KEY CONSIDERATIONS**

TRAVEL

International Travel
Travel to foreign countries—particularly those with a history of targeting U.S. technology—may warrant a security review to safeguard travelers and protect sensitive information.

High Risk Trigger

QUESTIONS TO ASK

- [ ] Is international travel involved in connection with this project, proposal, or contract?
- [ ] Is travel planned to a Foreign Country of Concern (FCOC)?
  - [ ] If yes, which country?
  - [ ] Who is traveling?
- [ ] Does the institution have a pre-travel approval system in place?
- [ ] Who is funding the travel?
  - [ ] If funded externally, does the funding source need to be disclosed as "other support" in a Conflict of Interest (COI) disclosure, depending on federal funder requirements?
- [ ] What is the purpose of the travel? (e.g., meeting collaborators, recruiting, presenting at a conference, being an invited speaker)
- [ ] What equipment or data will the traveler take?
  - [ ] Is the traveler bringing unnecessary data that could be exposed or stolen?
  - [ ] Can the traveler leave sensitive data at home?
  - [ ] Can the traveler use a clean laptop or only bring required materials on a USB drive?
- [ ] Does the destination country have encryption laws that could affect data or device security (e.g., China)?
- [ ] Will the traveler need to access the institution's IT network remotely during travel?
  - [ ] If yes, can remote access via VPN be avoided by bringing necessary materials on a secure, removable device (e.g., USB)?
- [ ] If attending a conference:
  - [ ] Who is hosting or sponsoring the conference?
  - [ ] Are any hosts, sponsors, or organizing committees listed on U.S. entity risk lists?
  - [ ] Could attending the conference create a perceived or real high-risk connection for the institution?
- [ ] If the traveler has authorized access to export-controlled (EC) programs:
  - [ ] Will any EC data be taken during travel?
  - [ ] Will the traveler present any part of an EC project?
  - [ ] If yes, is sponsor approval required for public disclosures?
  - [ ] Has proper written sponsor approval been obtained, if required?

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

INTELLECTUAL PROPERTY

Commercial / Proprietary Value or Controlled Distribution Agreements
Research that produces valuable intellectual property may require a security review to prevent misappropriation or unauthorized use by foreign entities.

Agreements requiring reviews may include:
- Licenses
- Material Transfer Agreements (MTAs)
- Data Use Agreements (DUAs)
- Memoranda of Understanding (MOUs)
- Patents

High Risk Trigger

QUESTIONS TO ASK

Commercial / Proprietary Value or Controlled Distribution Agreement
- [ ] Does the proposal, project, or contract involve proprietary intellectual property (IP), such as;
  - [ ] Patentable technologies
  - [ ] Licensable technologies
- [ ] Are there any nondisclosure agreements (NDAs) in place that could restrict the distribution of information?
- [ ] Are there publication restrictions in the agreement?
  - [ ] If so, was the sponsor's publication approval process followed?
  - [ ] Is there documentation of the required approvals?
- [ ] Has the agreement, NDA, contract, or Memorandum of Understanding (MOU) been routed through the appropriate office (e.g., Tech Transfer or Licensing Office) for review and approval?

Tech Transfer Considerations
- [ ] Does this review involve any agreements related to intellectual property, such as licenses, material transfer agreements (MTAs), data use agreements (DUAs), memoranda of understanding (MOUs), patents, or facility usage agreements that allow external partners to use institutional labs and resources?

DISCLAIMER
- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

1 EXTERNAL PROFESSIONAL ACTIVITIES TRIGGER ▶ **2 KEY CONSIDERATIONS**

EXTERNAL PROFESSIONAL ACTIVITIES

Conflict of Interest
It is essential to disclose all relevant information in proposals and publications to maintain research integrity and prevent potential conflicts or misuse.

Other Activities
Includes executive and professional roles, such as:

- Participation in Foreign Talent Recruitment Program (FTRP) or Malign FTRP
- Requests for remote work
- Conducting lectures, teaching, or serving on review panels
- Faculty appointments at foreign institutions
- Consulting or independent agreement with a foreign entity

High Risk Trigger

QUESTIONS TO ASK

Conflict of Interest

- [ ] What disclosures have been made regarding the project or funding?
- [ ] Are the disclosures current and up to date?
- [ ] Are screening reviews, such as for travel funding, being cross-checked with disclosures of other support?
- [ ] Does the travel reviewer have access to the Conflict of Interest (COI) disclosure or the necessary information to verify the disclosures?
- [ ] If outside funding for travel needs to be disclosed and has not been, who is responsible for contacting the traveler or researcher to address the oversight?

Other Activities

- [ ] Is the investigator participating in a Foreign Talent Recruitment Program (FTRP) or a Malign FTRP?
  - [ ] If so, can the relevant talent program documentation be requested to determine if it meets the definition of malign?
- [ ] Are there any requests for remote work?
- [ ] Is the investigator conducting lectures, teaching, or serving on review panels?
- [ ] Does the investigator hold a faculty appointment at a foreign institution?
- [ ] Is the investigator engaged in consulting or an independent agreement with a foreign entity?

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

VISITING SCHOLARS

Engagements Involving International Visitors
Includes:
- Hosting students, researchers, or visitors from outside the U.S.
- Inviting international collaborators
- Sponsoring visas for research personnel
- Processing visiting scholar requests

High Risk Trigger

QUESTIONS TO ASK

Engagements Involving International Visitors

- [ ] Will visiting scholars be involved or working on this project?
- [ ] Who are the visiting scholars?
- [ ] Does the institution have a specific definition of a "visitor" in terms of duration (e.g., any visit longer than 2 weeks)?
- [ ] Is the visitor financially supported by their original institution or by the host institution?
- [ ] Is the visitor bringing any additional family members? If so, were travel documents received for additional screening?
- [ ] What is the purpose of the visit (e.g., teaching, research, observation)?
- [ ] Will the visitor have access to any federally funded research?
- [ ] Does the visitor require access to any buildings, labs, or computer systems?
- [ ] Will the visitor be adjacent to or in close proximity to export-controlled research?
  - [ ] If so, do the export-controlled (EC) researchers need to be notified, and should they adjust their procedures to prevent information spillage?
- [ ] Does the visitor's background and expertise align with the purpose of the visit?
- [ ] Who is involved in the recommendation and approval process? Are proper stakeholders engaged?
- [ ] If the visitor is considered a risk, are there behavior monitoring tools in place to mitigate exposure?
- [ ] Does the visitor sign any official agreement binding them to follow the host institution's policies on computer usage, code of conduct, approved data sharing, or other legal concerns?

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

TECHNOLOGIES

Dual-Use Applications
Research with both civilian and military potential requires careful review to prevent misuse of data for defense or weapons-related purposes.

Critical & Emerging Technologies
Research in STEM or other emerging fields — especially those with dual-use potential — should undergo security review to evaluate associated risks.

High Risk Trigger

QUESTIONS TO ASK

Dual-Use Applications

- [ ] Are any Bureau of Industry and Security controlled technologies involved in this project or will they be used?
- [ ] If controlled equipment or data is utilized, do physical access controls meet the required standards?
- [ ] Does the cybersecurity environment meet the required standards for handling controlled equipment/data?
- [ ] How will the data be transferred, and is the transfer solution compliant with the required standards?
- [ ] Is dual-use equipment properly identified and inventoried?
- [ ] Do users and researchers understand when dual-use items are controlled and when they are not?
- [ ] Are they aware of any restrictions on foreign national access?
- [ ] How is appropriate access to dual-use equipment screened, authorized, and monitored?

Critical & Emerging Technologies

- [ ] Are any BIS-controlled technologies or emerging technologies involved in this project or will they be used?
- [ ] While emerging technologies may not have formal control requirements like export-controlled (EC) items, they should be treated with the same level of scrutiny if the unit or department maintains a culture of security.

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

ADMINISTRATIVE

Sabbatical or Leave of Absence
Faculty or staff on sabbatical or leave must ensure continuity of research activities and maintain compliance with institutional policies.

Sponsored Research Account (SRA)
Providing authentication credentials to individuals who are not employees may require special review.

Staffing
New faculty hires involved in sponsored research projects must undergo appropriate onboarding and compliance checks to align with project requirements.

High Risk Trigger

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

QUESTIONS TO ASK

Sabbatical or Leave of Absence

- [ ] Do you have a sabbatical or leave of absence planned?
- [ ] If the sabbatical is to a foreign country, is this a greater concern, particularly if it involves a Foreign Country of Concern (FCOC)?
- [ ] Is someone else taking over the person's research during their sabbatical or leave?
  - [ ] If so, does the sponsor need to be notified, and is there a need to modify the award to assign the new person?
- [ ] Is the person on leave responsible for supervising any official visitors?
  - [ ] If yes, who will take over the supervisory responsibility?
- [ ] Will the person leave their research behind or take data with them?
  - [ ] Can they be directed to leave the data behind?
- [ ] Will the person be accessing IT systems while on leave or sabbatical?

Sponsored Research Account (SRA)

- [ ] Are there any collaborators who will need institutional credentials as part of this project?
- [ ] Can their access be limited to only the required information, or do they have access to higher-level folders exposing them to projects they should not have access to?
- [ ] Are there behavioral monitoring tools in place to track access and downloads by collaborators?
- [ ] Do non-employees sign any legal agreements regarding cybersecurity procedures, such as proper use of institutional systems or NDAs?

Staffing

- [ ] What is the name and background of the new hire (education, work history)?
- [ ] Will the new hire be seen as having risky connections by federal funders?
  - [ ] Are new hires conducting federal research will be reviewed by the agency for potential risks?
  - [ ] Are new hires ensured compliant, to ensure that the institution is prepared for funding agency audits?
- [ ] Do HR or the hiring manager consult with Research Security (RS) for assistance in identifying malign foreign influence during the hiring process?
- [ ] Are risky collaborations terminated prior to employment, or are they properly disclosed on Conflict of Interest (COI) or Malign Foreign Talent Recruitment Program (MFTRP) forms?
- [ ] Do hiring managers consider the new hire's potential to secure federal funding as an asset?

BACK TO TRIGGERS

VIEW TOOLS & RESOURCES

1 OTHER TRIGGER ▶ 2 **KEY CONSIDERATIONS**

OTHER

Export and Other Controlled Data
Research involving controlled data, including export-restricted materials or technology.

Cybersecurity
Ensuring robust cybersecurity measures is essential to protect sensitive research data and prevent breaches.

Insider Threat Risk
Unauthorized access or misuse of research data by staff or collaborators.

International & State Data Protection
International or state data protection policies (GDPR, CCPA, etc) to be considered while collaborating.

High Risk Trigger

DISCLAIMER

- This list of considerations may not be comprehensive and is provided for informational purposes only. Additional considerations may require.
- Use these considerations at your own discretion, and always review any data or content before relying on it.

BACK TO TRIGGERS

QUESTIONS TO ASK

Export and Other Controlled Data

- [ ] Is there any controlled data involved in the project?
- [ ] What specifically is being protected: ITAR-regulated items or EAR-controlled technology?
  - [ ] ITAR: what is the category under the U.S. Munitions List?
  - [ ] EAR: what is the Export Control Classification Number?
- [ ] Are there any concerns regarding participation by foreign nationals?
  - [ ] If so, how does this affect the research team composition?
  - [ ] Does it impact the broader research environment (e.g., others in the area)? Are physical access controls needed?
- [ ] Are there any publication restrictions related to the project?
- [ ] Are cybersecurity controls required?
  - [ ] Where will controlled data be stored?
  - [ ] How will the data be transmitted or moved securely?
  - [ ] How will remote meetings be conducted to maintain compliance?
- [ ] Is a Technology Control Plan (TCP) required before the project can begin?
- [ ] Is additional training needed for researchers working with controlled data?

Insider Threat Risk

- [ ] Has the staff or collaborator involved in this project ever been prosecuted, investigated, or found guilty of espionage or similar offenses?
- [ ] Does the institution have an existing insider threat program associated with classified research that can be leveraged for unclassified research?
- [ ] Is there a formal, accessible method for reporting potential insider threats (e.g., anonymous ethics reporting systems)?
- [ ] Is there coordination between leadership to monitor and be alerted to employees with formal reprimands, poor performance reviews, or wage garnishments that could elevate insider threat risk?
- [ ] Does the institution's insider threat program include processes for monitoring staff or collaborators who have access to sensitive research data?

Cybersecurity

- [ ] Does the project involve any Controlled Unclassified Information (CUI)?
  - [ ] If yes, which parts of the project involve CUI?
- [ ] Where will CUI or other sensitive data be stored?
- [ ] How will CUI or sensitive data be transmitted or moved (e.g., email, file transfer)?
  - [ ] If emailing CUI, is the email system specifically compliant with applicable standards?
- [ ] Are there bulk data transfer requirements associated with the project?
- [ ] Is there a compliant Zoom, MS Teams or other collaboration platforms available for remote meetings involving CUI?
- [ ] Are researchers creating new CUI as part of this project, or are they only receiving it?
- [ ] Are System Security Plans (SSPs) needed for isolated or air-gapped systems?
- [ ] What cybersecurity certifications or verifications are in place for this project (e.g., NIST 800-171, 800-53, CMMC Level 2 or higher)?
- [ ] Is the project aligned with the institution's cybersecurity program, policies, and infrastructure?
- [ ] If applicable, has the cybersecurity compliance been independently verified or certified?

International & State Data Protection

- [ ] Are there any international, federal, or state data protection laws or policies that apply to this project and require compliance?
- [ ] If so, which specific regulations (e.g., GDPR, HIPAA, CCPA) are relevant, and what compliance measures need to be implemented?

VIEW TOOLS & RESOURCES

3 TOOLS & RESOURCES

INTRODUCTION

The Tools and Resources section equips users with the means to gather accurate and relevant information to support their assessments. It includes categorized lists of both open-source (free) and commercial (paid) tools aligned to each specific trigger, helping streamline data collection.

By integrating practical resources directly into the assessment workflow, this resource strengthens the connection between inquiry and evidence. It supports informed, defensible decision-making aligned with institutional and federal requirements.

HOW TO USE

- After reviewing a trigger and its key considerations, use this section to identify specific tools that can help you gather needed information. Each trigger has its own page listing relevant free and paid tools, making it easy to find the right resource for the activity you're assessing.

- These tools are grouped by trigger to minimize confusion and ensure quick access to the most applicable options. Use them to fill information gaps, validate disclosures, or crosscheck details. Always review the tool's current access, reliability, and data policies before use.

TARGET AUDIENCE

- Research Security Officer
- Principal Investigator
- Research Administration Support Offices

PURPOSE & BENEFITS

Increases Accuracy
Connects key questions to real data sources.

Institutional Flexibility
Can be tailored to internal policies, resource availability, and security posture.

Supports Tiered Risk Approach
Allows institutions to begin with free tools and scale to commercial ones as needed.

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS

VIEW ALL TOOLS

CONTINUE TO TOOLS & RESOURCES

COLLABORATIONS

International Collaborations
Collaborations with foreign partners — particularly in areas tied to national security — should be carefully reviewed to prevent unauthorized sharing of sensitive information and to ensure compliance with applicable regulations.

International Student Engagement
Includes mentoring, advising, or tutoring students not enrolled at the institution, as well as situations where former students continue remote work on sponsored projects after returning to their home countries.

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Controlled Unclassified Information (CUI) Review
- Current & Pending (Other) Support
- Cybersecurity SSPs
- Disclosure Systems
- Elsevier
- eRA Commons
- Foreign Talent Recruitment Program
- Google Scholar
- InfoEd
- Institutional Website
- Malign Foreign Talent Recruitment Program
- National Institutes of Health (NIH) Archives
- National Institutes of Health (NIH) PubMed
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- ResearchGate
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report

PAID / COMMERCIAL

- Academic Analytics
- Cayuse
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

FUNDING

Federal Funding
Research projects funded by U.S. government agencies may require a research security review.

Commercial Research Funding
Sponsored research supported by non-federal sources, such as commercial entities or non-profit research organizations.

International Sponsors / Foreign Source of Support
Research sponsored by organizations or entities based outside the United States.

Grant Funding with Restrictions
May include limitations on publishing, personnel eligibility, commercial NDAs, export controls, CUI involvement, or CMMC compliance requirements.

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Controlled Unclassified Information (CUI) Review
- Current & Pending (Other) Support
- Cybersecurity SSPs
- Disclosure Systems
- Elsevier
- eRA Commons
- Foreign Talent Recruitment Program
- InfoEd
- Malign Foreign Talent Recruitment Program
- National Institutes of Health (NIH) Archives
- Office of Sponsored Programs
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Sponsor's Website
- Technology Control Plans
- Time & Effort Certification Report

PAID / COMMERCIAL

- Academic Analytics
- Cayuse
- COEUS
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

TRAVEL

International Travel
Travel to foreign countries—particularly those with a history of targeting U.S. technology—may warrant a security review to safeguard travelers and protect sensitive information.

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- Cybersecurity SSPs
- Disclosure Systems
- Technology Control Plans
- Travel Registry

PAID / COMMERCIAL

- Academic Analytics
- Crisis24
- Dimensions
- FinchAI
- iSOS
- Kharon
- SAP Concur
- Strider
- Terra Dotta
- Visual Compliance

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

INTELLECTUAL PROPERTY

Commercial / Proprietary Value or Controlled Distribution Agreements
Research that produces valuable intellectual property may require a security review to prevent misappropriation or unauthorized use by foreign entities.

Agreements requiring reviews may include:
- Licenses
- Material Transfer Agreements (MTAs)
- Data Use Agreements (DUAs)
- Memoranda of Understanding (MOUs)
- Patents

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Intellectual Property Review Workflows
- Invention Disclosure Forms
- License Agreements
- Material Transfer Agreements
- Non-Disclosure Agreements
- National Institutes of Health (NIH)
- National Science Foundation (NSF)
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Tech Transfer Office
- Time & Effort Certification Report
- World Intellectual Property Organization (WIPO)

PAID / COMMERCIAL

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

EXTERNAL PROFESSIONAL ACTIVITIES

Conflict of Interest
It is essential to disclose all relevant information in proposals and publications to maintain research integrity and prevent potential conflicts of interest or misuse.

Other Activities
Includes executive and professional roles, such as:

- Participation in Foreign Talent Recruitment Program (FTRP) or Malign FTRP
- Requests for remote work
- Conducting lectures, teaching, or serving on review panels
- Faculty appointments at foreign institutions
- Consulting or independent agreement with a foreign entity

High Risk Trigger

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- 7 Sons of National Defense of China List
- Australian Consolidated List
- BioSketch
- Canada Named Research Organizations
- Center for Security and Emerging Technology
- CSET Chinese Talent Program Tracker
- Disclosure Systems
- Elsevier
- EU Consolidated List
- Foreign Talent Recruitment Program
- Malign Foreign Talent Recruitment Program
- National Institutes of Health (NIH) Archives
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report
- UK Consolidated List
- US BIS Consolidated List
- US NDAA 1260H List
- US NDAA 1286 List
- US OFAC Consolidated List
- US OFAC SDN List

PAID / COMMERCIAL

- Academic Analytics
- Cayuse
- Dimensions
- FinchAI
- Kharon
- Strider
- Visual Compliance

CONTINUE TO SUMMARY TEMPLATE SECTION

VISITING SCHOLARS

Engagements Involving International Visitors
Includes:

- Hosting students, researchers, or visitors from outside the U.S.
- Inviting international collaborators
- Sponsoring visas for research personnel
- Processing visiting scholar requests

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Elsevier
- Foreign Talent Recruitment Program
- Malign Foreign Talent Recruitment Program
- National Institutes of Health (NIH) Archives
- National Institutes of Health (NIH) PubMed
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report

PAID / COMMERCIAL

- Academic Analytics
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

TECHNOLOGIES

Dual-Use Applications
Research with both civilian and military potential requires careful review to prevent misuse of data for defense or weapons-related purposes.

Critical & Emerging Technologies
Research in STEM or other emerging fields — especially those with dual-use potential — should undergo security review to evaluate associated risks.

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Critical and Emerging Technologies List
- Export Control Office
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Time & Effort Certification Report

PAID / COMMERCIAL

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

ADMINISTRATIVE

Sabbatical or Leave of Absence
Faculty or staff on sabbatical or leave must ensure continuity of research activities and maintain compliance with institutional policies.

Sponsored Research Account (SRA)
Providing authentication credentials to individuals who are not employees may require special review.

Staffing
New faculty hires involved in sponsored research projects must undergo appropriate onboarding and compliance checks to align with project requirements.

High Risk Trigger

TOOLS & RESOURCES

FREE / OPEN-SOURCE

- BioSketch
- Consulting Agreements
- Contract Agreements
- Cybersecurity SSPs
- Employment Agreements
- Foreign Country of Concern
- InfoEd
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Time & Effort Certification Report

PAID / COMMERCIAL

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS | BACK TO CONSIDERATIONS | i

CONTINUE TO SUMMARY TEMPLATE SECTION

3 TOOLS & RESOURCES

COLLABORATIONS

FREE

- BioSketch
- Controlled Unclassified Information (CUI) Review
- Current & Pending (Other) Support
- Cybersecurity SSPs
- Disclosure Systems
- Elsevier
- eRA Commons
- Foreign Talent Recruitment Program
- Google Scholar
- InfoEd
- Institutional Website
- Malign FTR Program
- National Institutes of Health Archives
- National Institutes of Health PubMed
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- ResearchGate
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report

PAID

- Academic Analytics
- Cayuse
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

FUNDING

FREE

- BioSketch
- Controlled Unclassified Information (CUI) Review
- Current & Pending (Other) Support
- Cybersecurity SSPs
- Disclosure Systems
- Elsevier
- eRA Commons
- Foreign Talent Recruitment Program
- InfoEd
- Malign FTR Program
- National Institutes of Health Archives
- Office of Sponsored Programs
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Sponsor's Website
- Technology Control Plans
- Time & Effort Certification Report

PAID

- Academic Analytics
- Cayuse
- COEUS
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

TRAVEL

FREE

- Cybersecurity SSPs
- Disclosure Systems
- Technology Control Plans
- Travel Registry

PAID

- Academic Analytics
- Crisis24
- Dimensions
- FinchAI
- iSOS
- Kharon
- SAP Concur
- Strider
- Terra Dotta
- Visual Compliance

INTELLECTUAL PROPERTY

FREE

- BioSketch
- Intellectual Property Review Workflows
- Invention Disclosure Forms
- License Agreements
- Material Transfer Agreements
- Non-Disclosure Agreements
- National Institutes of Health (NIH)
- National Science Foundation (NSF)
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Tech Transfer Office
- Time & Effort Certification Report
- WIPO

PAID

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS

3 TOOLS & RESOURCES

EXTERNAL PROFESSIONAL ACTIVITIES

FREE

- 7 Sons of National Defense of China
- Australian Consolidated List
- BioSketch
- Canada Named Research Organizations
- Center for Security and Emerging Technology
- CSET Chinese Talent Program Tracker
- Disclosure Systems
- Elsevier
- EU Consolidated List
- Foreign Talent Recruitment Program
- Malign FTR Program
- National Institutes of Health Archives
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report
- UK Consolidated List
- US BIS Consolidated List
- US NDAA 1260H List
- US NDAA 1286 List
- US OFAC Consolidated List
- US OFAC SDN List

PAID

- Academic Analytics
- Cayuse
- Dimensions
- FinchAI
- Kharon
- Strider
- Visual Compliance

VISITOR SCHOLARS

FREE

- BioSketch
- Elsevier
- Foreign Talent Recruitment Program
- Malign Foreign Talent Recruitment Program
- National Institutes of Health Archives
- National Institutes of Health PubMed
- Open Researcher and Contributor ID (ORCID)
- PubPeer
- SciENcv
- Scopus
- Technology Control Plans
- Time & Effort Certification Report

PAID

- Academic Analytics
- Dimensions
- FinchAI
- IP Talons
- Kharon
- Strider
- Visual Compliance

TECHNOLOGIES

FREE

- BioSketch
- Critical and Emerging Technologies List
- Export Control Office
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Time & Effort Certification Report

PAID

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

ADMINISTRATIVE

FREE

- BioSketch
- Consulting Agreements
- Contract Agreements
- Cybersecurity SSPs
- Employment Agreements
- Foreign Country of Concern
- InfoEd
- Open Researcher and Contributor ID (ORCID)
- SciENcv
- Technology Control Plans
- Time & Effort Certification Report

PAID

- Academic Analytics
- Dimensions
- FinchAI
- Kharon
- Strider

DISCLAIMER

- This list of tools may not be comprehensive and is provided for informational purposes only.
- SECURE Center does not endorse or recommend any tool listed.
- Features, pricing (free or paid), and availability are subject to change by the providers, and SECURE Center is not responsible for those changes.
- SECURE Center does not guarantee the availability, accuracy, or performance of any tool.
- Use these tools at your own discretion, and always review any data or content before using.

BACK TO TRIGGERS

1 TRIGGERS ▶ 2 **ADDITIONAL TRIGGERS**

STUDIES

Pilot Studies or Feasibility Tests
Early-stage research may introduce unanticipated risks and should be reviewed to ensure proper oversight and alignment with institutional protocols.

SURVEYS

Online Survey Platforms
Collecting optional personal or demographic data as part of any online survey may require review.

DATASETS

Use of Deidentified Data Sets
Even with anonymized data, a review is recommended to assess the potential for reidentification or data linkage risks.

STUDENT PROJECTS

Student-Led Research in Capstone or Thesis Projects
Projects led by students may involve novel methods or populations and benefit from a risk review to ensure compliance and ethical integrity.

INTERNAL PROJECTS

Collaborative Projects with Other Departments
Cross-departmental collaborations can involve differing practices and data handling standards, warranting a risk assessment for alignment.

EVENTS

Hosting Public-Facing Events or Workshops
Events open to the public may involve participant data collection or interactions that introduce reputational or privacy risks.

INTERNAL COLLABORATIONS

Internal Collaborations and Institutional Research
Includes collaborations within the same institution and classroom-based or low-risk educational research settings, where institutional oversight is already in place.

RESEARCH TYPE

Theoretical and Literature-Based Research
Covers purely theoretical work, literature reviews, and meta-analyses that involve no data collection or participant interaction.

OPEN SOURCE DATA

Public and Open Source Data Use
Encompasses use of public domain data and open educational resources, where data is nonsensitive and freely accessible.

EXISTING PROTOCOLS

Approved or Reused Protocols
Applies to studies using previously approved, unchanged research protocols that have already undergone risk assessment.

TOOLS

Commercial and Off-the-Shelf Tools
Includes the use of widely available software or platforms without custom modifications or sensitive data use.

HANDLING

Low-Risk Materials and Sample Handling
Covers use of non-toxic, non-hazardous materials and small-scale handling of biological samples with minimal safety or regulatory concerns.

BACK TO TRIGGERS

4 RISK ASSESSMENT SUMMARY TEMPLATE

INTRODUCTION

The Risk Assessment Summary Template is a structured, fillable PDF designed to help research security professionals document and archive assessments in a consistent and comprehensive manner. It serves as the final step in the research risk assessment workflow, capturing key findings, due diligence steps, and supporting evidence.

This tool reinforces transparency and preparedness by ensuring institutions have clear records of how each potential risk was reviewed and addressed. It supports future audits, internal reviews, and compliance with evolving federal guidance.

HOW TO USE

- After identifying a trigger and reviewing the key considerations and relevant tools, use this template to formally document your assessment. The fillable fields are grouped by risk areas such as disclosures, funding, foreign affiliations, and visiting scholars.
- Complete the summary section at the top, followed by the applicable fields based on the scenario. Attach or reference any supporting documentation used during the assessment. Once filled, the form can be saved and archived as part of the institution's research compliance records.
- This outcome completes the cycle — moving from awareness (triggers), to investigation (key questions), to action (tool use), and finally to documentation for accountability and continuity.

TARGET AUDIENCE

- Research Security Officer
- Principal Investigator
- Research Administration Support Offices

PURPOSE & BENEFITS

Standardized Documentation
A consistent format for institutional recordkeeping.

Audit-Ready Reporting
Ensure key details are stored for future audits, reviews, or internal reporting.

Team Continuity
Create a lasting record that supports knowledge transfer during staff transitions.

Efficient Review Process
Enable structured reviews by summarizing relevant findings and actions in one place.

BACK TO TRIGGERS

BACK TO CONSIDERATIONS

VIEW RISK ASSESSMENT SUMMARY TEMPLATE

INTAKE

Unique ID

Proposal

Researcher / Visitor

First Name

Middle Name

Last Name

ORCID

Trigger

Sponsor Type

Sponsor Name

Supervisor / PI

Department / School

Country

Review Start Date

Review End Date

Reviewed By

RISK ASSESSMENT

Risk Assessment Determination

Restricted Party Screening

Risk Assessment Tool

Other Risk Assessment Tool

Summary

EDUCATION & EMPLOYMENT

Are there any flags for education & employment

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

DISCLOSURES

Are there any disclosures?

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

FOREIGN TALENT RECRUITMENT PROGRAM

Select program type

◯ None ◯ FTRP ◯ MFTRP

Supporting documentation

☐ Saved to folder

Notes

PUBLICATIONS / COLLABORATIONS

Are there any flags for publications / collaborations?

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

CRITICAL / EMERGING TECHNOLOGIES

Are there any flags for critical / emerging technologies

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

FUNDING SOURCES

Is there any funding?

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

PATENTS

Are there any patents?

◯ Yes ◯ No

Supporting documentation

☐ Saved to folder

Notes

Print Form | Save As... | Reset Form