ASCE

ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

Insider Threat Program Consideration at Institutions of Higher Education

April 7, 2022

Deb Kuidis, Kelly Hochstetler, Jessa Albertson, John Talerico, Garrett Eaton, Jonathan Snowden, Chris Jenkins, and Carl Taylor

INTRODUCTION

In January 2021, the National Science and Technology Council (NSTC), Office of Science and Technology Policy (OSTP), and Joint Committee on the Research Environment (JCORE) published *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise* ("*Recommended Practices*"). The publication surveyed twenty-one recommended measures that universities improve to optimize the benefits of a culture of open scientific inquiry and international collaboration while mitigating the risks posed by the efforts of certain non-US organizations intent on exploiting or inappropriately influencing federally funded research.

This paper examines two of these recommendations*:*

- *#13 Increase awareness and protections against circumstances and behaviors that may indicate a risk to research security*, and
- as part of *#4 Establish and operate a comprehensive research security program*, the insider threat awareness program.

Additionally, and in response to NSTC's January 2022 publication Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, this paper also addresses the "research security training" component of the requirements for research security programs as it pertains to insider threat training.

To be clear, the thoughts presented here are suggestions, and not directions, from university practitioners for additional consideration. No two academic institutions are identical, and each should develop and maintain strategies, policies, and processes that are consistent with its specific missions, research portfolios, policies, and state requirements.

OVERVIEW

Prevention and detection of insider threats, including education and awareness programs, has long been required for universities conducting classified research under the National Industrial Security Program (NISP) requirements for cleared facilities, however, this may be an unfamiliar concept to many in academia. For the purposes of this paper, we will use the following definitions:

> ***Insider*** - Any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.
>
> ***Insider Threat*** - The potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

While the idea of having a campus-wide Insider Threat Program (ITP) may be new or seem ill-suited for academic environments, the basic tenets are not particularly different in methodology or implementation to other types of risk identification, mitigation, and prevention programs that are common on university campuses for various forms of potential risk noncompliance. Examples of such programs include ones addressing fraud, waste, and abuse; crime/loss prevention; sexual harassment; personal/community safety; and research misconduct. Each program asks, and in some cases requires, people to watch for and report atypical, concerning, or suspicious behaviors that may indicate a threat to personal safety (e.g., physical, psychological, or emotional harm), the university (e.g., property, finances, or reputation), or the integrity of research (e.g., plagiarism, cyber intrusions, certain outside activities, commitments and affiliations). While those examples address different threats/risks, the behavioral indicators are often similar, and the programs all advocate reporting the behavior to the appropriate office/official. Other functional areas (e.g., human resources, procurement, information security, finance, or audit) within the university will likely have behavioral indicator lists you can use or adapt to assess insider threats/risks.

DISCUSSION

Universities may elect to leverage existing programs or create new ones to identify, report, and manage vulnerabilities, threats, and risks posed by insiders. Regardless of how the program is structured and where it resides within the institution, there are common high-level elements that should be considered and agreed upon: responsible executive, senior administrative/functional manager (senior manager), scope and intent of the program, procedures for managing reported or identified threats, and how to package/present the program to promote adoption and support.

We suggest that the responsible executive for the program be an official with oversight of the full scope of the ITP, typically a vice president/provost/chancellor, e.g., vice president for research if the scope is limited to the research enterprise. The responsible executive should assign a senior manager to lead (i.e., solely or principally responsible and accountable) or coordinate (e.g., distributed responsibility and accountability) the ITP. This may be a person with risk management, facility security, ethics/compliance, information security, counsel, or other responsibilities that indicate a position of trust. JCORE Recommend Practices recommendation #2 refers to this role as the "chief security officer."

Developing a clear statement of scope and intent is critical to developing an effective program. The opening sentence of JCORE Recommended Practices recommendation #13 provides a good starting point: increase awareness of and protections against circumstances that may indicate risk to research security and integrity. This statement should be customized to align with each university's scope of implementation as well as local naming conventions and culture. Scoping your program should consider applicable regulatory requirements, your university's risk profile and risk tolerance as well as available resources, including personnel time/effort. Phasing in a program based on predetermined risks and university leadership support, and then adapting as risks change and resources allow, is a strategy that will assist institutions in meeting their end goals for a program. One university may start small and narrowly define their scope (e.g., certain high-sensitivity federally funded or STEM research programs), then adapt as the risk environment, available resources, and regulatory requirements evolve. Other universities, for example those with classified or export-controlled research, may decide to expand an existing ITP to cover additional risk areas, research, and researchers. Programs that are not tailored to an institution’s unique profile may result in resources being spread too thin or loss of support and credibility.

An appropriately scoped and resourced ITP supports an institution’s research community and protects its research against improper influence and exploitation that has the potential to threaten the integrity and security of the research environment or community. When building support for the program, it is important to remember that issues of foreign influence, insider threats, and research security may be extremely sensitive, and some members of the research community may feel unfairly targeted, especially by foreign influence concerns. These concerns should not be taken lightly. Extreme care must be taken to ensure that programs comply with all policies and regulations regarding discrimination and privacy and do not create an unsafe or unwelcoming environment for your institution’s community. Focusing programmatic elements on identifying behavioral indicators as opposed to individual characteristics may help alleviate concerns and increase adoption of the program. Policies, processes and procedures must guard against overreach and be followed consistently across the program demonstrating objectivity to avoid singling out individuals.

Some universities may find framing insider threat programmatic elements as a research data risk prevention program to be an effective approach. At others, it may be more in keeping with institutional culture to focus on career/reputation management. It may also be helpful to stress the benefit that behavioral indicators may be signs of undue stress or pressures which may lead an individual to commit research or professional misconduct, fraud, or other illegal or unethical actions and for which the university may have resources to assist with these concerns such as employee counseling programs.

Goals and Objectives of an institution’s program

Institutions should consider the following goals and objectives for an ITP working group:

1) Gather, integrate, and report relevant and available information indicative of potential or actual threats, anomalies, “red flags” to research integrity, data, information or technology, misuse of property and information technology networks, and other issues / programs under its responsibility dictated in a charge by executive leadership.

2) Serve as a platform to evaluate, investigate, report, and mitigate potential insider threats.

3) Serve as an opportunity to identify, respond, and intervene to actions and behaviors from individuals before they develop into an insider threat risk.

4) Identify appropriate education and awareness training for personnel assigned duties associated with conducting research.

Education and Awareness Training

The ITP will include a training program to conform to the NSPM-33 Implementation Guidance to educate university personnel on what constitutes an insider threat, identifying behavioral indicators, how the institution is addressing the risk and resources for help or additional information. This training program should consist of:

a. **Initial Training:** Initial training and outreach that describes the program is a key component for establishing credibility and building support. This training should be tailored to an institution's risk profile and program. Cleared institutions may find the Center for Development of Security Excellence (CDSE), Insider Threat computer-based training for employees at NISP universities helpful.

b. **Refresher Training**: Refresher training can be developed by the senior manager for the university that reinforces the principles and resources from the initial training. NISP requires cleared universities to conduct annual training for insider threat to cleared employees; however, non-NISP universities can set a frequency consistent with their level of risk and established policies and procedures. Individual universities may utilize a homegrown training regimen or the CDSE Inside Threat training, though approval may be required by the Defense Counterintelligence and Security Agency (DSCA) Industrial Security Representative for cleared universities.

Outside Assistance available

a. National Insider Threat Task Force (NITTF) from Office of the Director of National Intelligence, and the Department of Homeland Security has numerous resources and training materials available.
b. Cybersecurity & Infrastructure Security Agency (CISA) Insider Threat Mitigation Resources.
c. Each university is encouraged to have an open dialog with their local Federal Bureau of Investigation (FBI) Office, and other agencies that are appropriate for their institution.
d. Cognizant Security Agency (CSA) for NISP universities.
e. Other counterintelligence agencies, such as Naval Criminal Investigative Services, Army Counterintelligence, and Air Force Office of Special Investigations
f. Local law enforcement, which is typically contacted through the Campus Police Department.
g. State law enforcement and/or other agencies for training resources, and incident review/vetting

ITP Components that routinely exist at an institution

There are existing processes, systems, or policies already in place at your institution that are components of an ITP that can be used as a foundation for a program to successfully identify behavioral indicators and risks associated with an insider threat, such as:

- Institutional Research Compliance
  - Export control reviews and/or disclosures
  - Conflict of Interest (COI)/Conflict of Commitment (COC)
  - Environmental Health and Safety (EHS) lab authorizations, audits, and incidents
  - Animal and Human subjects (IRB) oversight committees
- Investigation teams (which may exist within General Counsel, Compliance, Internal Audit, Public Safety, Security Management Offices, Cyber Security Offices)
- Whistleblower Hotlines
- Research Integrity Offices or officers
- Human Resources procedures meant to address behavioral issues, disciplinary actions hiring/termination actions
- Sexual Misconduct or Title IX policy oversight
- Information technology and Cybersecurity steps already being taken to monitor network activity

- Department of Energy Reactor and Facility Requirements
- Select Agent / Biosafety Level (BSL) Requirements
- Section 117 of the Higher Education Act of 1965 reporting procedures
- Visiting scholar procedures
- Institutional travel oversight and management programs
- Emergency response committees or groups, particularly with respect to threats of physical harm such as active shooter situations[1]
- Federal agency partnerships, including federal law enforcement

Given these existing areas, universities can focus their ITP on coordinating these separate functions and cultivating a leadership team or Insider Threat Working Group (ITPWG) properly trained and prepared to identify, review, and adjudicate vulnerabilities, "red flags", anomalies, and threat information. The ITPWG could also advise and assist the senior manager on programmatic development, such as training, outreach/communication, record keeping, etc.

There may be additional options available to your institution, based on organizational culture, resources, applicable requirements and risk tolerance.

Composition of the ITPWG

The composition of each institution's ITPWG should reflect the entirety of the goals and objectives as established by the responsible executive and group membership can vary. Also, each institution must consider the dynamics and/or challenges that arise from the number of participants. However, within the context of addressing research security, best practices are to consider the following functional area representatives, either as full or ad hoc members:

1) ITP senior manager and, if the institution is a cleared contractor, the Facility Security Officer (FSO). (Security violations, vulnerabilities, compromises, and other issues)
2) Human Resources. (Hiring actions, discrimination concerns, identify workplace issues, concerning work habits, foreign employment and travel, termination actions, and financial issues)
3) IT and IT Security. (Identify unusual data transfers, poor cyber hygiene, unusual network activity, and other anomalous foreign and domestic activity)
4) Export Control Officer. (Restricted party collaborations, foreign travel, regulatory violations, "red flags" and anomalies)
5) Research Compliance and Integrity. (non-compliance with compliance programs such as IRB, Select Agent, nuclear, and other Federal agency programs, issues or anomalies with Conflicts of Interest & Commitment, including foreign employment)
6) General Counsel. (Provides legal and policy interpretation and assistance)
7) Chief Security Officer for the institution if position exists. (Investigations, risk mitigation strategies and courses of action, interaction with senior leadership, coordinates with outside agencies including local and federal law enforcement)

[1] While threats such as active shooters are likely outside the cognizance of a research-focused ITP, the authors wish to call attention to the importance of universities accounting for such threats. Department of Homeland Security has many valuable resources that may aid in training and awareness around active shooter events, such as Active Shooter - How to Respond (dhs.gov).

8) Institutional Public Safety or Police Department. (Identify law enforcement issues, incidents and encounters with the community of the institution, coordination with external agencies if necessary)
9) Immigration/International Affairs.
10) Consider faculty representation/leadership (familiar with research environment and has unique insight into research activity and personnel. May help identify behaviors that are truly abnormal and not normal course of academic or research activity)
11) Consider Internal Audit, Risk Management (identifying anomalies, quantifying and communicating risk to executive leadership)
12) Intellectual Property/Technology Transfer, to identify and review potential licensees for any concerns regarding misuse or possible theft of intellectual property.
13) Research Administration, assess individual's sponsored research portfolio to address risks or disclosure needs to sponsors, especially those requiring foreign interest disclosures

The membership suggestion and capabilities/responsibilities may vary per institution, so this list is not all inclusive. In addition, broader objectives beyond JCORE Recommended Practices may require additional membership. Leadership of the ITPWG will also vary depending on the institution. It's recommended that the ITPWG member leading the group is appointed by executive leadership with clear responsibility and authority.

Identification of Risk areas that are a concern of leadership (risk assessment)

Insider threat risk exists whether the institution or individuals engage in domestic activities, international, or both. When assessing the institutional and individual risks, there are several in which areas university administration and research faculty should evaluate the risks. Chart 1 below highlights just some of the areas where this threat may exist:

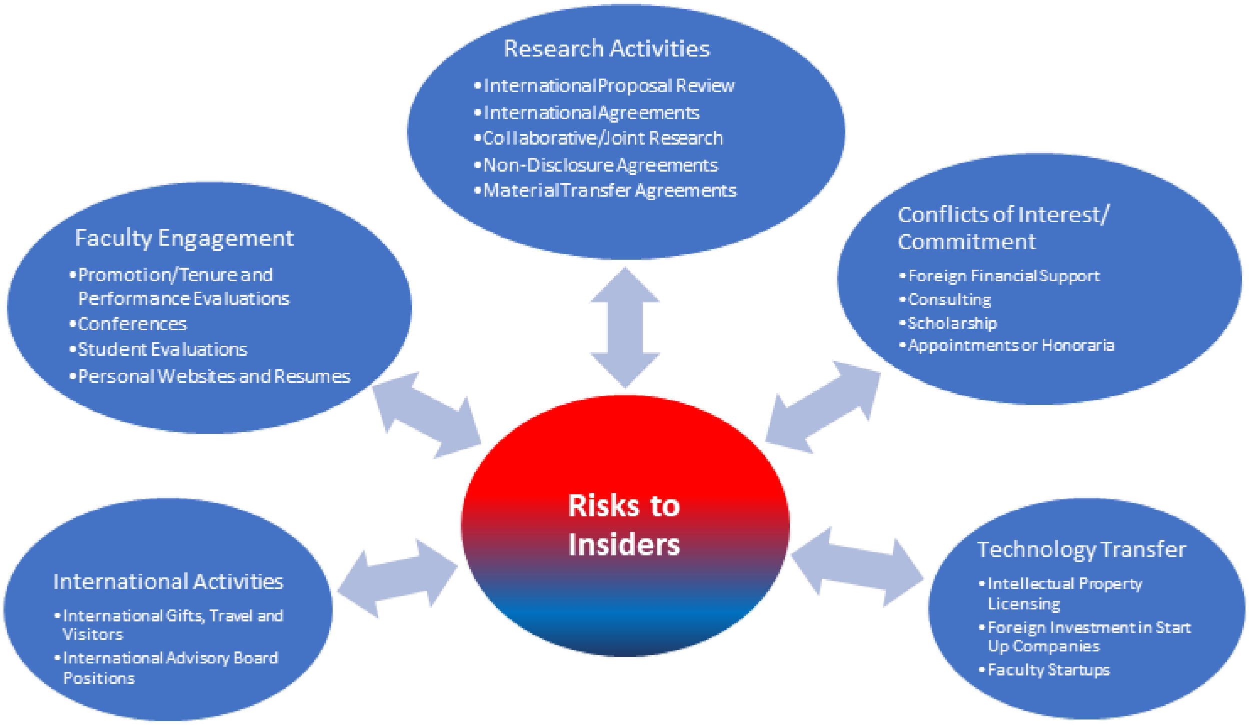
Research Activities
•International Proposal Review
•International Agreements
•Collaborative/Joint Research
•Non-Disclosure Agreements
•Material Transfer Agreements
Faculty Engagement
•Promotion/Tenure and Performance Evaluations
•Conferences
•Student Evaluations
•Personal Websites and Resumes
Conflicts of Interest/ Commitment
•Foreign Financial Support
•Consulting
•Scholarship
•Appointments or Honoraria
Risks to Insiders
International Activities
•International Gifts, Travel and Visitors
•International Advisory Board Positions
Technology Transfer
•Intellectual Property Licensing
•Foreign Investment in Start Up Companies
•Faculty Startups

Chart 1: Insider Threat Risk Areas at Universities

Information Sharing and Assessments

University administrative activities are generally a dispersed set of functions and responsibilities, which complicates information sharing at times. University leadership needs to first assess which departments/offices on their campuses hold responsibilities over the areas they deem to be at risk and create processes by which information can be easily shared amongst those groups to conduct a comprehensive insider risk assessment. Leadership could use Chart 1 or other criteria to identify where valuable information may reside in different areas of the university. The ITPWG previously mentioned could function as an organization to identify these risk indicators.

Methodology for Review – Analysis – Notifications

Institutional policy or procedures should be clear on when, how, and to whom a potential insider threat should be reported. Upon receipt, each report must be assessed promptly to determine if it is a credible and actionable insider threat. Cross-functional coordination may be necessary to redirect reports made to the incorrect office and for reports implicating multiple compliance areas or functions, which should be part of the assessment and procedures identified by the senior manager and/or ITPWG.

Once a report of a potential insider threat is deemed credible, the responsible person should take immediate action to protect institutional assets, notify appropriate personnel (e.g., leadership, counsel, compliance officers, CIO, etc.), and initiate an investigation. The focus of the investigation should be to understand the cause, method, scope, and impact of the incident and to identify areas for improvement. These findings should be reported to the responsible executive by way of the senior manager.

Insiders have authorized access, know where information is stored, and often know the strengths and weakness of policy and systems. Application of this knowledge by the insider may slow or prevent detection by institutional control measures. Insiders, even those without malice, may cause significant damage by not following policies and procedures or through simple carelessness. Institutions need a holistic approach to the insider threat with the right people, policies, and technology in place to protect valuable personnel, facilities, systems, technology, data, and institutional reputation.

Effective and risk-based insider threat management requires the organization to identify, locate/track, and assign relative values to its assets in order to prioritize assessment of anomalies, individual behavior, and "red flags" and, when needed, take timely action to safeguard high value resources. Key members of the institution should be responsible for proactively identifying critical areas of concern and the associated assets that would degrade the organization's ability to accomplish their goals and objectives. Special attention should be given to records and files, electronic or hard copy, containing sensitive data (e.g., U.S. government classified and controlled unclassified information; personally identifiable information that could be used for identity theft; payment card information; non-public research data/results and other institutional or third-party intellectual property).

Investigations

Conducting an insider threat investigation often requires extensive use of internal resources. Many institutions have established policies, procedures and/or processes for investigations. Using these for insider threat incidents helps ensure efficient use and prioritization of resources. Cross-functional consistency in the conduct, reporting, and communication of investigations will likely be appreciated by executive leadership and may help identify common threads that can and should be addressed at an institutional level.

Most universities have individuals or groups with valuable institution-specific experience conducting investigations and who are familiar with applicable institutional policies (e.g., information security, export controls, facilities management, audit, financial compliance, counsel, human resources, etc.). The ITPWG and senior manager should consider leveraging these individuals or groups when engaging in an insider threat investigation in the effort to utilize resources most efficiently. For example, it may be necessary to involve legal counsel early in the investigation to invoke privileged conversations or public relations prior to an employment or law enforcement action that may become public. The best practice is always to keep knowledge of ongoing investigations limited to those who truly have a "need to know".

Individuals who investigate incidents or reports should be identified and trained in applicable policies and procedures in advance. The individual(s) or team investigating an incident should understand their authorities, scope of the investigation, responsibility to protect the integrity of the investigation as well as the privacy of the subject(s) of the investigation.

External Reporting of Potential Insider Threats

If an investigation results in the need to report any findings outside the university, the insider threat procedures should be clear on how and who will make such reports. When reporting on behalf of an institution, questions about appropriate jurisdiction should be addressed by counsel, the senior manager, and the ITPWG.

External reporting/notification varies depending on the institution and specific incident or allegation but may include local, state, or federal law enforcement; Defense Counterintelligence Security Agency (DCSA) for NISP universities; the Directorate of Defense Trade Controls or Bureau of Industry and Security; or a federal research sponsor. These agencies may provide guidance on evidence collection or request that the institution take or delay taking specific actions.

Always take appropriate internal actions to protect personnel, facilities, and the integrity of information technology systems and networks per policy, and state and federal laws.

CONCLUSION

There are many tools and resources both internal and external to universities to help identify, reduce, and mitigate insider threat risks to universities. Due to the special emphasis and concerns from the U.S. Government on protecting the research environment from improper influence and exploitation, university research enterprises are a good place to begin an ITP. Appropriately scoped and resourced ITPs will support the outward engagement, both domestic and international, that is essential to rapid innovation, superior education, and technical superiority while protecting people, facilities, technology, missions, and their reputations.

APPENDICES, etc.

REFERENCES

Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Enterprise (Jan 2021). https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf.

Cybersecurity & Infrastructure Security Agency (CISA) website.

- Defining Insider Threats. https://www.cisa.gov/defining-insider-threats.
- Detecting and Identifying Insider Threats. https://www.cisa.gov/detecting-and-identifying-insider-threats.

Insider Threat Indicators Overview. National Insider Threat Special Interest Group. https://www.nationalinsiderthreatsig.org/itrmresources/Insider%20Threat%20Indicators%20Overeview.pdf.

Spotting Insider Threats. Federal Bureau of Investigation, U.S. Department of Justice. https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf

Insider Threat. Domestic Security Alliance Council website. https://www.dsac.gov/topics/insider-threat.

National Security Presidential Memorandum 33 (NSPM-33). https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security for United States Government-Supported Research and Development, January 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
National Insider Threat Task Force (NITTF) Resource Library website. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-resource-library/briefings-to-the-insider-threat-community

Cybersecurity & Infrastructure Security Agency (CISA) Insider Threat Mitigation Resources website. https://www.cisa.gov/publication/insider-threat-mitigation-resources

Acknowledgement

This product was developed by the Academic Security and Counter Exploitation (ASCE) Working Group. The working group was established to tap the expertise of universities that have demonstrated excellence in academic security and counterintelligence programs in an effort to help address threats of espionage at, or inappropriate exfiltration from U.S. academic institutions.

The group includes a variety of universities, from those that conduct only fundamental research to those that conduct classified research on behalf of the federal government.

You can receive additional information about the Academic Security and Counter Exploitation Program and request membership information by emailing ASCEP@tamus.edu.