The National Academies
Office of Program Security, Insider Risk Management Program

The Insider Threat Program: Quick Reference Guide

Below are a few key questions everyone should be able to answer about The Insider Threat Program at the National Academy of Sciences.

WHAT IS AN "INSIDER THREAT PROGRAM"?

An Insider Threat Program is required by the U.S. government to establish a process for centralized analysis, reporting and response to potential threats before they damage our Nation and organization. Our program here at the National Academies is the "Insider Risk Management" program and is designed to detect, deter, respond to, and mitigate any events that may occur as a result of an Insider Threat. Our Insider Threat Senior Official is Enita Williams and the program is staffed by the Office of Program Security.

WHAT IS AN "INSIDER THREAT"?

An Insider Threat is "the potential risk that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S." (NISPOM, Appendix C). This can include damage to the national security of the U.S. or the National Academies through espionage, sabotage, unauthorized disclosure/use of national security information, or the unauthorized disclosure/use of controlled unclassified information.

WHAT DOES THE INSIDER THREAT PROGRAM MEAN FOR YOU?

Under the program, we each have a responsibility to report to the proper officials any indicators or behaviors that may compromise the security of the institution, its work, or its personnel.

INDICATORS & BEHAVIORS	HOW TO REPORT
• **Espionage, Sabotage, Terrorism, or Subversive Activity;** • **Suspicious contacts (esp. involving foreign nationals)** • **Loss, Compromise, or Suspected Compromise of Classified Information or Controlled Unclassified Information** • **Information Spillage** • **Unauthorized Access to IT systems, spaces, or information that you are not authorized to receive and do not have a contractually-based need-to-know** • **Surveillance (e.g. of individuals or buildings)**	Send written report to the Insider Threat Program Senior Official (Please do not include classified information in your report.) Written reports may be submitted via email to insiderriskmgmt@nas.edu or anonymously via Insider Risk Management Dropboxes. • Keck: Located on the 2nd Floor, Wall Across from Meeting Room 206 • NAS: Located in Basement, Wall outside of Office 058
• **Information System Misuse/Abuse**	
• **Change In Personal Status (e.g. change in name, outside employment, etc.)** • **Abuse of prescription drugs, alcohol, or use of illegal substances** • **Hospitalization for mental or emotional disorders (where the individual is a threat to themselves or others);** • **Financial issues - sudden unexplained affluence or excessive indebtedness (e.g. garnishments, bankruptcy, foreclosures, liens, judgments, delinquent taxes, etc.)** • **Criminal Activities.**	

All insider threat indicators/behaviors should be reported to the proper officials to mitigate risks. A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be evident and require reporting.

Enita Williams
Insider Threat Program Senior Official, Office of Program Security, ewilliams@nas.edu, (202) 334-3292

Kamilya Kamilova
Security Manager, Office of Program Security, kkamilova@nas.edu, (202) 334-2634

The National Academies
Office of Program Security, Insider Risk Management Program

The Insider Threat Damage

An Insider Threat can cause serious damage to our organization, to our nation's economic competitiveness, and to national security. Harm can come in the form of: leaks, spills, espionage, sabotage, and fraud.

TYPES OF DAMAGE AN INSIDER THREAT CAN CAUSE

A **Leak** is when a trusted insider intentionally releases classified or sensitive information to an unauthorized person(s) or to the public.	This is not whistleblowing – within the classified and restricted information environment, there are proper channels by which whistleblowing can be accomplished without compromising the information or national security.
A **Spill** (**Information Spillage**) refers to instances where sensitive information (e.g., classified information, export-controlled information, controlled unclassified information) is inadvertently placed on information systems that are not authorized to process such information.	**Spills** occur in a number of ways including: • Improper marking of classified information • Classification by compilation • Failure to use authorized information systems • Failure to confirm declassification guidance
Espionage is a national security crime; specifically, it violates Title 18 USC, §§ 792-798. Espionage convictions require the transmittal of national defense information with intent to aid a foreign power or harm the U.S. However, even gathering, collecting, or losing national defense information can be prosecuted under Title 18.	**Economic Espionage** is defined under §1831 of Economic Espionage Act of 1996 and comprises behavior that denies the rightful owner of the economic benefit of property that the owner has gone to reasonable means to protect and does so with the intent to benefit a foreign entity. **Trade Secret Theft** is defined under §1832 of the Economic Espionage Act of 1996 and covers the conversion of a trade secret to the economic benefit of anyone other than the rightful owner. There is no requirement for a foreign nexus in Trade Secret Theft.
Sabotage is the act of hampering, deliberately subverting, or hurting the efforts of another or an institution. It is most often an issue in the context of military law, when a person attempts to thwart a war effort, or in employment law, when disgruntled employees destroy employer property.	**IT Sabotage** is when a trusted insider intentionally exceeds or misuses an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the organization, or the organization's data, systems, and/or daily business operations.
Fraud is when an insider uses company information, resources, or systems to make a false representation of a matter of fact—whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed—that deceives and is intended to deceive another.	**FOR QUESTIONS OR ASSISTANCE CONTACT:** *Enita Williams* Insider Threat Program Senior Official, Office of Program Security (202) 334-3292 *Kamilya Kamilova* Security Manager Office of Program Security (202) 334-2634