LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

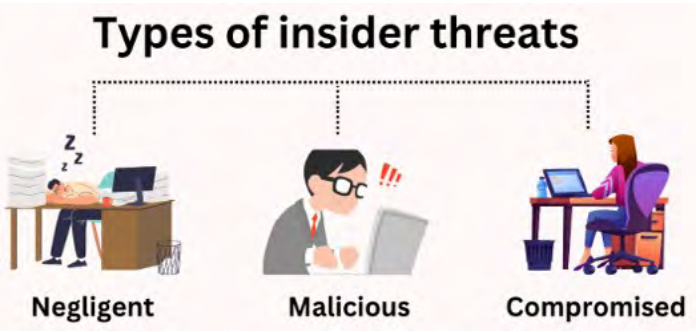
SEPTEMBER 2025

INSIDER THREAT

What Is an Insider Threat:

An insider is any person with authorized access to any United States Government resource, such as personnel, facilities, information, equipment, networks, or systems. Their access can come through employment, a contractual relationship, or volunteer activities. Anyone with access can be an insider threat.

An insider threat occurs when an insider uses her or his authorized access, whether intentionally or not, to harm the security of the United States. This can be accomplished through espionage, terrorism, unauthorized disclosure, or the loss or degradation of department resources or capabilities.



What Are Adversaries:

Our adversaries include foreign governments, terrorist organizations, competitors, and non-state actors. They want to know non-public information that an insider can provide. This includes information related to:

- Personnel
- Methodologies, capabilities, and limitations
- Facility locations worldwide
- The countries the organization works with

Being aware of what information our adversaries want helps you protect your organization.

Collection Methods:

Examining past cases reveals that adversaries commonly use certain collection methods. Understanding these methods can help you identify the presence of a threat. The methods used in over 80% of cases are:

- Requests for information
- Academic solicitation
- Suspicious network activity
- Foreign visits
- Solicitation and marketing or seeking employment
- Targeting at conferences, conventions, and trade shows
- Elicitation and recruitment

Don't forget that insiders know about your organization's security controls, and how they might be able to work around them, to achieve their malicious objectives. A malicious insider may be conducting their own security assessment to determine the best method to achieve their objectives before the organization discovers the vulnerabilities.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

Statistics and Sourcing:

DOD INSIDER THREAT INCIDENTS From 2020 To 2024

- **U.S. Army Civilian Employee Sentenced to Prison for $100 Million Fraud Scheme / Used Funds For Jewelry, Clothing, Vehicles, Real Estate**—July 23,2024

  Janet Mello worked as a financial program manager for the U.S. Army at the Installation Management Command – G9 (Morale, Welfare and Recreation) Child and Youth Services (CYS) at Fort Sam Houston, in Texas. In or around December 2016 through at least August 29, 2023, Mello ran a business called Child Health and Youth Lifelong Development (CHYLD). The sole purpose of CHYLD was to receive grant funds from the 4-H Military Partnership Grant program, which Mello fraudulently secured by way of her position as a CYS financial program manager. Once Mello received a grant check, she deposited the check into her bank account and later spent the money on clothing, jewelry, vehicles, and real estate. Mello repeated the process 49 times during a six-year period, requesting approximately $117,000,000 in payments, and receiving approximately $108,917,749.

  - United States Department of Justice. (2024, January 25). Former Army civilian employee sentenced to 15 years in federal prison for $100 million fraud. https://www.justice.gov/usao-wdtx/pr/former-army-civilian-employee-sentenced-15-years-federal-prison-100-million-fraud

- **4 U.S. Army Depot Officials & Vendors Sentenced to Prison for $7 Million+ Contracting & Bribery Scheme**— September 13, 2022

  Jimmy Scarbrough was the equipment mechanic supervisor at the Red River Army Depot (RRAD) in Texarkana, Texas, from November 2001 until May 2019. Scarbrough directed more than $7 million in purchases from RRAD to RRAD vendor Jeffrey Harrison and Justin Bishop through the government purchase card (GPC) program. In order to manipulate the GPC program, which is designed to ensure a competitive bidding process, Scarbrough told the vendors what to bid, including the item, the quantity, and the price. By collecting fake bids from multiple vendors, Scarbrough was able to direct RRAD purchases to Harrison and Bishop while maintaining the appearance of a competitive bidding process. Scarbrough also defrauded the United States by falsely certifying that he had received the purchased items, therefore causing the RRAD to pay his select vendors. However, the reality was that Scarborough instructed the vendors not to deliver certain RRAD-purchased items. Scarbrough demanded hundreds of thousands of dollars in bribes from his selected vendors. Scarbrough accepted these bribes in various forms, including at least $116,000.00 in U.S. Postal Service money orders from Harrison. Scarbrough also had Harrison and Bishop purchase at least $135,000.00 in car parts or services for his hot rod collection, which included a red and black 1936 Ford Tudor, an electric green 1932 Ford Coupe, a cherry red 1951 Ford F-1 truck, and more. Scarbrough received more than $27,000.00 worth of firearms from Bishop, including rare Colt handguns and Wurfflein dueling pistols. Finally, Scarbrough directed at least $32,000.00 in donations to the Hooks Volunteer Fire Department while he was the Captain of Operations. In total, Scarbrough received more than $300,000.00 in bribes from Harrison and Bishop. Scarbrough is not the only official at RRAD who accepted bribes. Devin McEwin accepted more than $21,000.00 in bribes from Harrison, including hunting trips, donations directed to the Annona Volunteer Fire Department, and the refurbishment of his 1964 Ford truck. Louis Singleton accepted more than $18,000 in bribes from Harrison and others, including tickets to the Hall of Fame section of AT&T Stadium for the Dallas Cowboys football game against the New England Patriots. Singleton was the supervisor of the GPC program at the RRAD and was responsible for approving purchases requested by Scarbrough.

  - United States Department of Justice. (2022, March 29). Four Red River Army Depot officials and vendors sentenced in federal bribery and procurement fraud scheme. https://www.justice.gov/usao-edtx/pr/four-red-river-army-depot-officials-and-vendors-sentenced-federal-bribery-and