

LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

SEPTEMBER 2026

INSIDER THREAT AWARENESS MONTH

Insider Threat: More Than a Security Issue

When most people hear the term *insider threat*, they often think of espionage or someone intentionally stealing classified information. In reality, insider threats are much broader. Many incidents begin with ordinary employees experiencing personal, financial, or workplace stress, not individuals who intended to cause harm.

The Department of Defense Insider Threat Program was established to **detect, deter, and mitigate risks before they become security incidents. Rather than focusing solely on punishment, Insider Threat Programs are designed to identify employees who may need assistance while simultaneously protecting national security, organizational assets, Controlled Unclassified Information (CUI), Federal Contract Information (FCI), proprietary information, and classified material.

Early reporting allows organizations to intervene before concerning behaviors escalating into security incidents.

Understanding Insider Threats

An “insider” is anyone with authorized access to an organization's facilities, information, systems, equipment, or networks through employment, contract support, or volunteer activities.

An “insider threat” occurs when that trusted access, whether intentionally or unintentionally, is used in a way



that could damage national security, organizational operations, or protected information.

- Not every insider threat is malicious.
- Many incidents result from negligence or human error.
- Carelessness can be just as damaging as intentional misconduct.

Examples include:

- Mishandling classified information
- Improper handling of CUI
- Sharing sensitive information through social media
- Unauthorized removal of documents
- Connecting unauthorized devices
- Sending sensitive information to the wrong recipient

Every employee has a role in preventing these incidents.

Recognizing Common Risk Factors

An “insider” is anyone with authorized access to an organization's facilities, information, systems, equipment, or networks through employment, contract support, or volunteer activities.



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com



- Personal Stress
 - Divorce or family problems
 - Financial hardship
 - Mental or emotional distress
 - Substance abuse
- Workplace Indicators
 - Declining performance
 - Disciplinary actions
 - Working unusual hours without authorization
 - Significant behavioral changes
 - Expressions of anger or retaliation
- Technical Indicators
 - Accessing information outside assigned duties
 - Downloading excessive amounts of data
 - Using unauthorized removable media
 - Introducing unauthorized software or hardware
 - Attempting to bypass security controls

A single indicator DOES NOT necessarily mean someone poses a threat. However, multiple indicators together may warrant reporting so trained professionals can evaluate the situation fairly and objectively.

Adversaries Often Target Trusted Employees

Foreign intelligence services, competitors, cybercriminals, and other adversaries understand that trusted insiders already possess authorized access. Common collection techniques include:

- Social media recruitment
- Fake employment opportunities

- Academic collaboration requests
- Conference networking
- Suspicious requests for information
- Foreign travel contacts
- Phishing emails
- Cyber intrusions

Remember: If someone unexpectedly asks detailed questions about your work, systems, customers, projects, or technologies, treat the request with caution and report suspicious contacts according to organizational procedures.

Many espionage cases begin with what appears to be an innocent conversation.

Reporting Protects Everyone

One of the strongest messages throughout the CDSE training is that reporting is about helping, not accusing. Employees are ****not expected to investigate**** or determine whether someone is guilty of misconduct. Instead, employees should:

- Observe
- Document what they witnessed
- Report facts
- Allow the Insider Threat Program to assess the situation

Many reported employees ultimately receive assistance through Employee Assistance Programs (EAP), Human Resources, or supervisory support rather than disciplinary action. Early intervention frequently prevents both personal crises and security incidents.



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

What Should Be Reported?

Reportable concerns may include:

- Unauthorized attempts to access information
- Working outside normal hours without approval
- Suspicious foreign contacts
- Unreported foreign travel (where applicable)
- Unusual copying or downloading of files
- Use of unauthorized USB devices
- Requests for information outside an employee's responsibilities
- Significant unexplained behavioral changes
- Security violations involving classified information, CUI, or proprietary information

When in doubt, report the behavior—not your opinion.

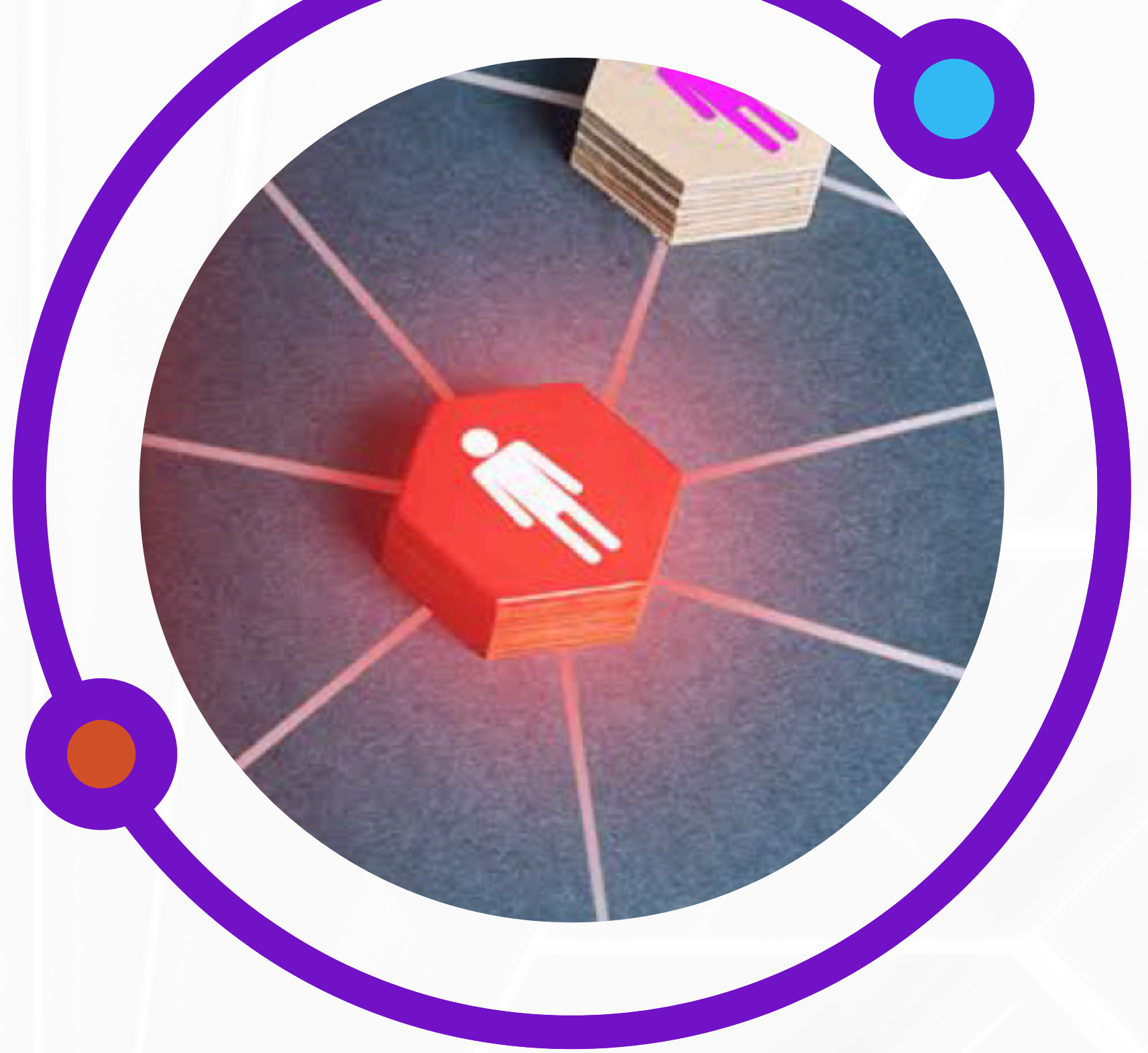
IMPORTANT Reminder!!!

Security is everyone's responsibility. Every employee serves as the organization's first line of defense against insider threats. Reporting concerning behavior DOES NOT mean someone is guilty. It allows trained security professionals to evaluate the situation, protect sensitive information, safeguard coworkers, and provide assistance when appropriate. Your vigilance helps protect:

- National Security Information
- Controlled Unclassified Information (CUI)
- Federal Contract Information (FCI)
- Intellectual Property
- Organizational Reputation
- Fellow Employees

Read at your own leisure:

- U.S. Department of Justice, Office of Public Affairs. (2026, January 12). Former U.S. Navy sailor sentenced to 200 months for spying for China. <https://www.justice.gov/opa/pr/former-us-navy-sailor-sentenced-200-months-spying-china>
- U.S. Department of Justice, U.S. Attorney's Office for the District of Maryland. (2026, June 26). Former U.S. National Security Advisor, John R. Bolton II, pleads guilty to violating the Espionage Act. [U.S. Department of Justice](https://www.justice.gov/opa/pr/former-us-national-security-advisor-john-r-bolton-ii-pleads-guilty-to-violating-the-espionage-act)
- Federal Bureau of Investigation, Washington Field Office. (2026, May 14). FBI Washington Field Office announces \$200,000 reward for information leading to apprehension of former U.S. counterintelligence agent charged with espionage for Iran. <https://www.fbi.gov/contact-us/field-offices/washingtondc/news/fbi-washington-field-office-announces-200000-reward-for-information-leading-to-apprehension-of-former-us-counterintelligence-agent-charged-with-espionage-for-iran>
- National Security Agency. (2026, April 7). NSA supports FBI in highlighting Russian GRU threats against routers. <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/>



Security Tip of the Month

Think – Protect – Report

Before taking any action involving sensitive information, ask yourself:

- Do I have a legitimate need-to-know?
- Am I following approved security procedures?
- Would this action create unnecessary risk?
- Should I report something I've observed?
- When something doesn't seem right, trust your instincts and follow your organization's reporting procedures. Together, we create a safer and more secure workplace.



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com