LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

MARCH 2026

COUNTERINTELLIGENCE AWARENESS: EVERYONE HAS A ROLE IN PROTECTING NATIONAL SECURITY

Counterintelligence (CI) is not limited to intelligence agencies or investigators. It is a shared responsibility across the cleared workforce. At its core, counterintelligence involves identifying, understanding, and mitigating threats posed by foreign intelligence entities, insider threats, and other adversaries seeking to exploit sensitive information, personnel, or systems.

Today's threat environment is increasingly complex. Adversaries no longer rely solely on traditional espionage methods. Instead, they employ cyber intrusions, social engineering, financial incentives, professional networking, and social media to gain access to sensitive information. These efforts are often subtle and designed to appear legitimate, meaning individuals may be targeted without realizing it.

Counterintelligence awareness is essential because informed employees serve as a critical line of defense. Recognizing threat indicators and knowing when and how to report concerns helps protect individuals, organizations, and mission objectives.

The Modern Counterintelligence Threat

Foreign intelligence services are persistent and adaptive. Their objective is often not immediate access to classified information, but the gradual development of trust and access. This may include cultivating professional relationships, offering career or financial opportunities, requesting seemingly harmless information, or leveraging travel and personal relationships to establish influence.

Common CI threats include foreign intelligence collection, insider threats that may be intentional or unintentional, and cyber enabled espionage such as phishing or credential harvesting. Adversaries may also exploit personal vulnerabilities including financial stress, workplace dissatisfaction, or social isolation.

Even information that appears insignificant on its own can become valuable when combined with other data. This is why all personnel, regardless of role, must remain vigilant.

Recognizing Counterintelligence Indicators

CI awareness includes recognizing behaviors or situations that may signal a potential threat. While a single indicator does not automatically imply malicious intent, patterns or repeated behaviors should raise concern.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

Examples include unreported or suspicious foreign contacts, pressure to bypass security procedures, requests for information outside an individual's need to know, or attempts to elicit information through casual conversation. Other indicators may include unexplained affluence, unusual foreign travel, or sudden changes in behavior or work habits.

Employees are encouraged to trust their instincts. If an interaction feels inappropriate or inconsistent with security expectations, it should be reported.

Reporting Is Preventive and Protective

Reporting counterintelligence concerns is not punitive. It is protective. Early reporting allows security professionals to assess risk, provide guidance, and address issues before harm occurs. In many cases, reporting helps protect employees from exploitation or coercion.

Timely reporting supports the protection of sensitive information, strengthens organizational security, and ensures compliance with national security requirements. Security professionals handle these matters discreetly and professionally.

Your Role in Counterintelligence

Every employee plays a role in counterintelligence by following security policies, maintaining awareness of threat tactics, safeguarding sensitive information, and reporting concerns promptly. Limiting work related discussions to authorized settings and adhering to need to know principles are essential daily practices.

If You see Something, Say Something

If you encounter a situation that raises counterintelligence concerns, or if you are unsure whether something should be reported, contact your Security team for guidance.

Protecting national security starts with awareness, and awareness starts with each of us.

References:

- Defense Counterintelligence and Security Agency (DCSA). *Counterintelligence Awareness and Reporting*.
- National Counterintelligence and Security Center (NCSC). *Foreign Intelligence Threats to U.S. Organizations*.
- Department of Defense. *Insider Threat Program Guidance*.
- Office of the Director of National Intelligence (ODNI). *National Counterintelligence Strategy*.