LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

APRIL 2024

NATIONAL SUPPLY CHAIN INTEGRITY

LIS Solutions (LIS) is committed to fighting against foreign intelligence entity (FIE) threats. Therefore, LIS employees have a duty and responsibility to protect multiple forms of sensitive information such as Controlled Unclassified Information (CUI), personally identifiable information (PII), and critical infrastructure information.

The National Counterintelligence and Security Center (NCSC) provides best practices to identify and assess the risks, as well as how to promote training and awareness. With the help of NCSC, we can effectively shield organizations from (FIE) threats.

FIE focuses on three main outcomes:

1. Identify foreign intelligence threats and share threat information.
2. Safeguard sensitive information, assets, and activities.
3. Prevent and detect insider threats.

There are high-level opportunities and challenges that FIE's wants to gain access to that pose an emerging risk and threat to U.S. National Security.

The National Counterintelligence and Security Center (NCSC) prioritizes its industry outreach efforts with U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that determine whether America remains the world's leading superpower or whether it becomes eclipsed by strategic competitors in the next few years.

The primary sectors include, but are not limited to:

1. Artificial intelligence (AI)
2. Bioeconomy
3. Autonomous Systems
4. Quantum Physics
5. Semiconductors

After being mandated by Congress, the NCSC's mission is to conduct counterintelligence (CI) outreach with the support of U.S. private sector, academic and research communities, and external stakeholders. The primary objective is to train and educate everyone with information about FIE intelligence threats so that they can identify and reduce any associated risks.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

THE MAIN THREAT TO U.S. INTELLIGENCE

The People's Republic of China (PRC) goal is to achieve leadership in various emerging technology fields by 2030. The PRC is the primary strategic competitor to the United States because it has a well-resourced and comprehensive strategy to acquire and use technology to advance its national goals. This includes technology transfers and intelligence gathered through its Military-Civil Fusion Policy and a National Intelligence Law that requires all Chinese entities to share technology and information with the PRC military, intelligence, and security services.

Beijing is focused on technologies it deems critical to its economic and military future, including enabling technologies such as biotechnology, advanced computing, and artificial intelligence. To help achieve the PRC's strategic goals, they utilize a wide variety of legal, quasi-legal, and illegal methods to acquire technology from the United States. These methods include but are not limited to:

- Intelligence services
- Science and technology investments
- Academic collaboration
- Joint ventures
- Mergers and acquisitions
- Non-traditional collectors (including co-opted insiders)
- Talent recruitment programs
- Research partnerships
- Front companies
- Legal and regulatory actions

To learn more about this topic, watch the video below at your leisure:
https://www.fbi.gov/news/stories/economic-espionage

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