Protect Your Organization from the Foreign Intelligence Threat

Introduction by Michael J. Orlando, Senior Official Performing the Duties of the Director of NCSC

Today the global threat environment is more diverse and dynamic than ever. As spelled out in the latest Annual Threat Assessment of the U.S. Intelligence Community (IC), a growing number of state actors and non-state actors are targeting the United States. They are no longer just interested in obtaining classified U.S. secrets but also are collecting information from almost all U.S. Government agencies and virtually every sector of the U.S. economy. Personal data, trade secrets, intellectual property, technology, and research and development are all being targeted by adversaries who have the capabilities, patience, and resources to get them.

To achieve their objectives, foreign adversaries are employing a range of illegal techniques, including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all these methods. They are also using a variety of legal and quasi-legal methods, including mergers and acquisitions, investments, joint ventures, partnerships, and talent recruitment programs to acquire U.S. technology and innovation. Ultimately, they seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions and ideals.

This new form of conflict is not fought on a foreign battlefield, but in our power grids, our computer networks, our laboratories and research facilities, our financial institutions, our healthcare providers, and our federal, state, local, and tribal governments. This battle will not be won by weapons and warriors, but by public and private sector partnerships and through American dedication and diligence.

This document is designed to provide public and private-sector organizations with an overview of counterintelligence (CI) and security best practices to help guard against foreign intelligence threats. The document includes links to risk mitigation materials that can help organizations improve their physical security, personnel security, operations security, cybersecurity, defensive CI, insider threat mitigation, and supply chain risk management.

Michael J Orlando

Intelligence Community Campus, Bethesda, Maryland

What is the Threat from Foreign Intelligence Entities?

The term "foreign intelligence entity" refers to a known or suspected foreign state or non-state organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes foreign intelligence services–defined as state intelligence services–and also can pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations.[1]

Regional adversaries and ideologically motivated entities, such as hackers and public disclosure organizations, also pose a growing threat to the United States. These actors have been able to advance their goals through the proliferation of more advanced and commercially available cyber and surveillance technologies.

The National CI Strategy of the United States of America 2020-2022 spells out three principal trends that characterize the current and emerging threat environment:

Their Methods

- Elicitation: The use of conversation to extract information, either in person, by email, on the phone, or through social media.
- Social Engineering: The impersonation of others to seem legitimate and surreptitiously acquire passwords or other key data.
- Economic Espionage: The theft or misappropriation of a trade secret with the intent or knowledge that the offense will benefit a foreign entity.
- Human Targeting: The targeting of individuals with access to sensitive information, who, for example, might unexpectedly meet someone who shares their interests or seeks an ongoing relationship.
- Cyber/Technical: Digital technologies used to compromise or acquire information stored or transmitted electronically.

- The number of threat actors targeting the United States is growing
- These actors have an increasingly sophisticated set of intelligence capabilities at their disposal and they are employing them in new ways to target the United States
- Threat actors are using these capabilities against an expanded set of targets and vulnerabilities

In short, today's threat environment no longer is characterized by the traditional spy-versus-spy game played by competing state intelligence services. It has evolved to include a broader range of actors using a wider variety of tools, both licit and illicit, to collect against a broader set of targets. These threat actors are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to acquire sensitive information, research, and technology from the U.S. economy as well as to gain access to our critical infrastructure. Threat actors also are conducing malicious influence campaigns that employ cyber operations, media manipulation, and political subversion to sow divisions in our society, undermine confidence in our democratic institutions, and weaken our alliances.

[1] NCSC, National Threat Identification and Prioritization Assessment, 2018.

How Do We Counter the Threat?

The National CI Strategy of the United States of America 2020-2022 spells out five strategic objectives for the U.S. Government in countering these threats. In addition to addressing its core CI mission of protecting classified information and facilities, the strategy dictates that the U.S. Government should:

- Protect the nation's critical infrastructure
- Reduce threats to key U.S. supply chains
- Counter the exploitation of the U.S. economy
- Defend American democracy against foreign influence
- Counter foreign intelligence cyber and technical operations

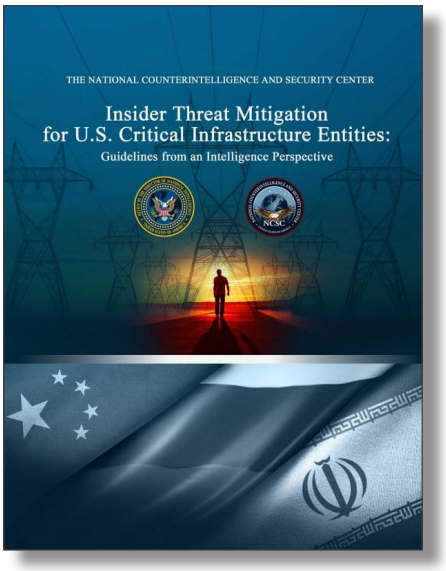
The strategy recognizes the U.S. Government cannot address these threats alone, but needs the assistance of the private sector, an informed American public, and our allies. Sound CI and security procedures must become part of everyday American business practices. The U.S. Government needs the private sector at its side combating these threats.

"The United States is entering into a period of intensifying strategic competition with several rivals, most notably Russia and China. Numerous statements from senior U.S. Defense officials make clear that they expect this competition to be played out primarily below the threshold of major war—in the spectrum of competition that has become known as the gray zone."

—RAND Corporation, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War,* 2019

What Steps Can Organizations Take?

A Common Understanding



The first step is a common understanding of the threat landscape. While adversaries are using increasingly complex, multi-pronged techniques to target organizations, they are all working to achieve basic human goals. Threat actors operate in both the physical and virtual worlds, but threat activity is not unique to either domain. Malicious actors in cyberspace represent key threats to organizations in the virtual domain, but humans inside an organization who wittingly or unwitting harm their organization (insider threats) can pose just as grave a threat. An entity may have world-class cyber defenses, but it is still vulnerable without an effective insider threat program. Comprehensive efforts to counter foreign adversarial threat should, therefore, address both the physical and cyber worlds and the humans and machines operating in each.

Traditional Security Practices

Both the public and private sectors are familiar with and practice traditional security disciplines. From deploying gates and guards, to using reference and background checks, to enhancing passwords and firewalls, to making available reporting mechanisms for employees, basic security practices remain essential to countering adversarial threat. NCSC and its partners offer several guides and practices to help build and strengthen traditional security practices.

- **Physical Security:** The Department of Homeland Security (DHS)-led Interagency Security Committee (ISC) is charged with enhancing the effectiveness of non-military federal facilities in the United States. They offer many physical security policies, standards, and best practices, including risk management practices to the public and the private sector.

- **Personnel Security:** As the primary support element enabling the Director of National Intelligence to execute her Security Executive Agent authorities, the NCSC Special Security Directorate (SSD) works with all federal agencies on the development and implementation of personnel security policy guidance for the federal national security workforce. SSD also works through the National Industrial Security Program Policy Advisory Committee and through other targeted outreach efforts to share policy guidance with private sector partners representing cleared contractor organizations.

- **Cybersecurity:** The goal of cybersecurity is to ensure the integrity, confidentiality, and availability of organizational systems, networks, and data. Many resources are available to help organizations enhance their cyber resilience and security. Cyber-related government and industry standards can be found at the National Institute of Standards and Technology (NIST). Additional cyber resources can be found at the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation (FBI), and the National Security Agency.

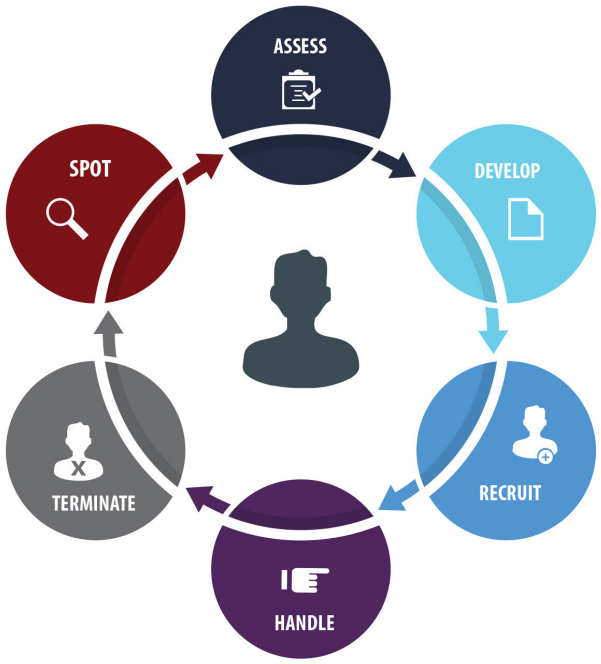
- **Operations Security (OPSEC):** OPSEC is a process by which an organization identifies its critical assets and information, assesses threats, vulnerabilities, and the impact of potential loss, evaluates risk, and then deploys countermeasures in a continuous cycle to effectively mitigate those risks. NCSC serves as the mission manager for the National OPSEC Program (NOP) and provides training and awareness materials for public and private sector partners. The NCSC NOP also provides liaison and assistance, governance and advocacy, and research and analysis for federal partner organizations.

CI Practices

CI can be defined as information gathered and activities conducted to protect against espionage, to protect other intelligence activities, and to prevent sabotage or assassinations conducted by or on behalf of foreign government or elements thereof, foreign organizations, or foreign persons or international terrorist activities.

Traditionally, CI has been viewed as primarily an Intelligence Community or military practice, i.e., "spy versus spy." Contrary to this perception, CI is critical to both public and private sector organizations as they work towards an enterprise-wide effort to protect against foreign intelligence entities. In today's world, where adversaries threaten America's critical infrastructure, economy, and the global information ecosystem, the threat from foreign intelligence entities requires strong public-private partnerships.

The Recruitment Cycle



A critical part of successful CI is understanding how foreign intelligence entities operate in the most basic form, such as targeting and developing human assets (witting and unwitting) to advance their agendas. Traditional intelligence services conduct this activity through the Recruitment Cycle: Spot, Assess, Develop, Recruit, Handle, and Terminate (cease handling the asset).

NCSC and its partners offer many resources to help organizations develop appropriate CI awareness campaigns to inform their workforces. These include the NCSC Know the Risk, Raise your Shield campaign and Safeguarding Our Future materials, and the Think before You Link materials developed by the United Kingdom's Centre for the Protection of National Infrastructure. In addition, the Department of Defense's Center for the Development of Security Excellence has resources and training available for CI awareness, including information on foreign intelligence entity collection methods and foreign travel threats. Furthermore, the FBI has numerous CI resources available for public and private sector partners.

Protecting Against the Insider Threat

Insider threats are individuals with authorized access to an organization's information, facilities, personnel, or other resources who use that access to wittingly or unwittingly cause harm to the organization. Insider threats can commit acts of corporate or traditional espionage, unauthorized disclosure, fraud, theft, sabotage, and even workplace violence. Trusted insiders may commit these negative acts on their own or they may be co-opted or exploited by foreign adversaries.

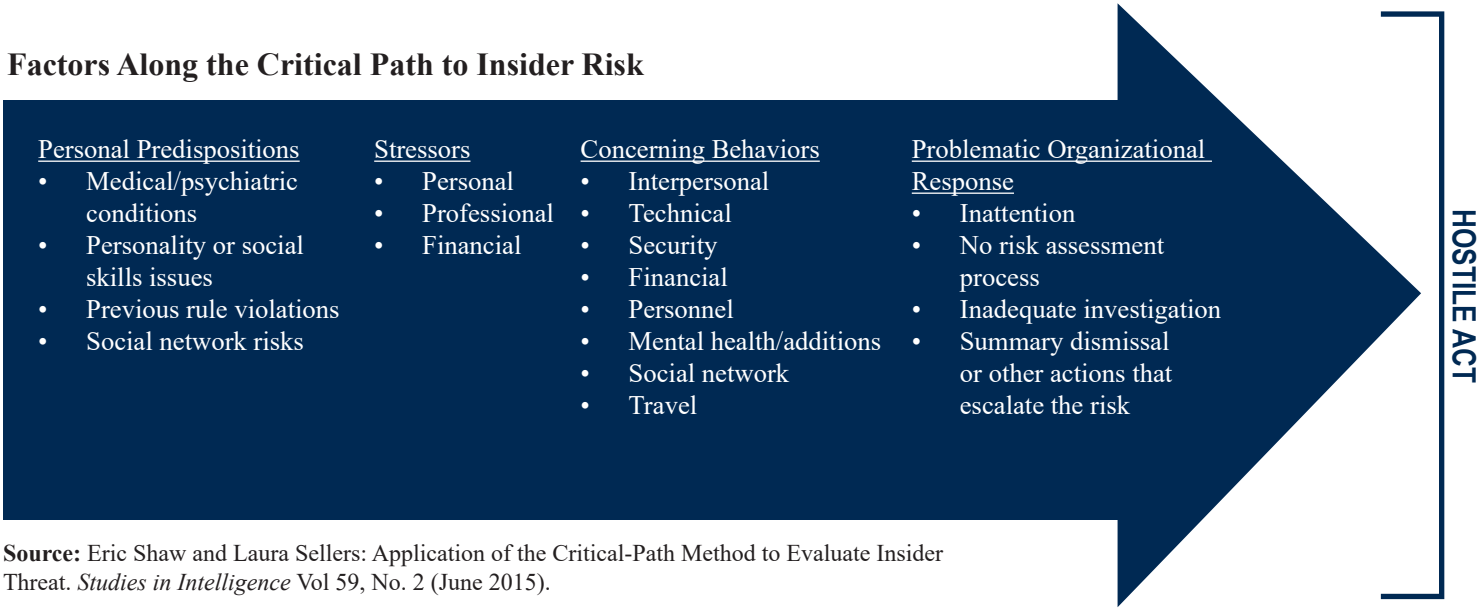
Executive Order 13587 requires all Executive Branch departments and agencies with access to classified information to develop an insider threat program in accordance with National Insider Threat Program Policy and Minimum Standards. Formal insider threat programs are a best practice for private and public sector organizations, regardless of access to classified information.

Countering insider threats is a whole-of-organization effort. The traditional security practices detailed above, combined with effective hiring practices, training and awareness campaigns, workforce wellness and support efforts, and the promotion of positive workplace culture and organizational trust are all essential elements of effective insider threat programs.

Insider threat programs are multi-disciplinary efforts that focus on proactive risk mitigation and information sharing while protecting the privacy and civil liberties of the workforce. Effective insider threat programs leverage resources across an organization, such as human resources and employee assistance programs, cybersecurity, traditional security, CI, legal and others, to identify anomalous behaviors that indicate an employee may be headed on a critical path toward harm. These programs then facilitate appropriate organization action to address the behavior, often resulting in positive outcomes for both the individual and the organization.

NCSC, the National Insider Threat Task Force, and their partners offer a wealth of resources, information, guides, and awareness materials to help organizations establish and improve insider threat programs.

Factors Along the Critical Path to Insider Risk



Source: Eric Shaw and Laura Sellers: Application of the Critical-Path Method to Evaluate Insider Threat. *Studies in Intelligence* Vol 59, No. 2 (June 2015).

Supply Chain Risk Management

The exploitation of key supply chains by foreign adversaries, especially when executed in concert with cyber intrusions and insider threat activities, represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure. Foreign adversaries are attempting to access our nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance–by a variety of means. NCSC offers multiple resources on supply chain risk management.

A supply chain risk occurs when the capability and intention of an adversary aligns with the opportunity to exploit a vulnerability. This scenario could allow an adversary to extract intellectual property, sensitive government data, and personally identifiable information. It could also allow an adversary to surveil, deny, disrupt, or otherwise degrade a component, system, or service, thereby adversely affecting critical industrial control systems, services, and products.

The increasing reliance on foreign-owned or controlled hardware, software, or services, as well as the proliferation of networking technologies, including those associated with the Internet of Things, creates vulnerabilities in our nation's supply chains. By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry. They also could subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis. For these reasons, supply chain security must be a priority in the acquisition process.

Tools and Technologies to Protect Each Stage of the Supply Chain Lifecycle

CONTENT & DESIGN

Zero Trust Architecture:
- Firewalls
- Data Encryption
- Continuous Monitoring

Validation & Verification

MANUFACTURING & INTEGRATION

Unique Product ID
- Barcodes
- Radio Frequency ID (RFID)
- Digital Markers

Zero Trust Architecture

DEPLOYMENT

Tamper-Evident Tapes & Seals
GPS, Bluetooth Tracking

MAINTENANCE

Access Controls
Zero Trust Architecture

RETIREMENT

Asset Management
Data Destruction Tools

How Do We Put it All Together?

Viewing Risk at an Enterprise Level

The fundamental risk management principle of identifying an organization's "crown jewels" is featured in the Physical Security guidance of the ISC, in DHS's critical infrastructure protection doctrines, in NIST's Risk Management Framework for Cybersecurity, and in supply chain risk management and OPSEC processes.

To effectively mitigate risk to critical assets, organizations should:

- Ensure a "crown jewel" assessment is conducted across the organization
- Consider threats to the organization's crown jewels from both human and cyber means
- Take into account adversary capabilities and intentions
- Develop an integrated risk management strategy that engages all threat mitigation practices in a coherent and coordinated manner to proactively avert harm
- When appropriate, include contractors, subcontractors, and suppliers in the risk mitigation process

Engage All Stakeholders and Promote an Organizational Culture of Awareness

Protecting an organization is not solely the duty of security personnel; everyone in the organization must play a role. Human resource programs are key partners in promoting and protecting the workforce from insider threat. Supervisors and managers are the first line of defense and response. Financial officers and acquisition/procurement staff play a critical role in supply chain risk management. Legal and contracting staff are essential in protecting sensitive information and intellectual property.

The key to it all is an informed workforce—including government and contractor personnel–that works together. For the private sector, this means including in your security awareness and risk mitigation efforts part-time and temporary staff, as well as vendors, suppliers, and other partners who have access to your facilities, information, and personnel.

Physical, Personnel, Cyber, Insider Threat, CI, Supply Chain Risk Management, and Operations Security programs are all well-developed, specialized disciplines in their own right. However, when these programs operate independently or are stove-piped in an organization, adversaries are often able to defeat them easily.

To more effectively mitigate risk, the best practices and protocols identified above must be fully ingrained into organizational culture, operational programs, and corporate policies, practices, and procedures. Countering foreign intelligence threats requires an integrated approach across the organization to ensure both human and technical threats are addressed in a coordinated, holistic manner, and that all security disciplines operate together seamlessly.

One of NCSC's core missions is to support and partner with organizations by providing subject matter experts, reference materials, and advocacy activities to help them create an integrated approach to countering foreign adversarial threats. For additional information on NCSC awareness information or materials, visit NCSC or follow us on Twitter at @NCSCgov, or on LinkedIn.