Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

October 18, 2018

The National Counterintelligence and Security Center (NCSC): An Overview

Section 3.5(a) of Executive Order 12333, The U.S. Intelligence Community, defines counterintelligence (CI) as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

Counterintelligence is often visible through its results: the July 2018 criminal indictment of Russian nationals and companies for interfering in the 2016 presidential election, and the October 2018 arrest and extradition of a Chinese intelligence officer for attempting to commit economic espionage are two examples. Less visible are efforts by U.S. counterintelligence elements to prevent cyber hacking and economic espionage, defend critical networks and infrastructure, and deter insider threats.

The National Counterintelligence and Security Center (NCSC) is one of the four mission centers within the Office of the Director of National Intelligence (ODNI). It was established in 2014 to lead United States CI and security activities by consolidating existing CI and security offices and responsibilities "to effectively integrate and align counterintelligence and security mission areas under a single organizational construct." NCSC develops and coordinates national CI strategy, policy, analytical products, priorities and budgets through a cadre of CI and law enforcement professionals from across the IC. Although NCSC oversees the CI and security activities of departments and agencies, it is not authorized to conduct investigations or operations, or to develop contacts with foreign intelligence services.

A National CI and Security Enterprise

PDD-75

Presidential Decision Directive (PDD) 75, *U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century*, signed by President Clinton on January 5, 2001, provided a foundation for a national organization to lead CI and security activities across the government. PDD-75 elaborated policy to keep pace with the proliferation of threats to U.S. national security that came with major developments in technology. PDD-75 also provided for the development of national CI strategy and policy, and the prioritization of CI requirements. Most importantly, PDD-75 provided for the formal establishment of a national CI and security organization, headed by the National Counterintelligence Executive (NCIX) and supporting office (ONCIX), a National CI Board of Directors, and a National CI Policy Board (NCIPB) to advise the NCIX on the CI strategy and policy. The CI structural elements established by PDD-75 were subsequently codified into statute through the Counterintelligence Enhancement Act of 2002. (P.L. 107-306, Title IX, §901(b), November 27, 2002, 116 Stat. 2432).

National CI Executive (NCIX)

As the senior official in the CI community, the NCIX is nominated by the President and, as of 2015, is also confirmed by the Senate. The 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), enacted to implement many of the recommendations of the National Commission on Terrorist Attacks upon the United States (known as the *9/11 Commission*), reorganized the NCIX and ONCIX within the newly constituted ODNI to facilitate the integration and coordination of national CI activities across the IC. With the consolidation of national CI and security activities in the NCSC in 2014, the NCIX was redesignated as the Director, NCSC.

Resources

The NCSC and CI and security programs for each IC element are funded through the National Intelligence Program (NIP) budget. The Director of National Intelligence (DNI) manages the NIP in order to align resources with prioritized requirements through the iterative Intelligence Planning, Programming, Budgeting, and Evaluation (IPPBE) process. See CRS In Focus IF10428, *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*, by Michael E. DeVine.

NCSC Strategic Goals and Statutory Functions

The NCSC *Strategic Plan* for 2018-2022 specifies five strategic goals:

1. Advancing knowledge of and ability to counter foreign and other threats.
2. Protecting United States critical infrastructure, technologies, facilities, classified networks, sensitive information and personnel.
3. Advancing the CI and security mission, and optimizing CI cooperation and partnerships.
4. Engaging and advocating for government and private stakeholders to improve effectiveness.
5. Achieving organizational excellence.

To achieve these goals, NCSC has a number of statutory functions, including these:

- Producing the National Threat Identification and Prioritization Assessment (NTIPA), a strategic planning document with a consolidated list of CI requirements tied to specific CI threats.

- Producing and implementing a national strategy derived from the NTIPA's assessment of the CI environment.
- Overseeing and coordinating the production of analyses of CI incidents, including damage assessments and lessons learned.
- Coordinating the development of CI and security budgets for departments and agencies with responsibility for CI and security activities.
- Developing CI and security priorities for investigations and CI operations.
- Conducting outreach programs to government and private sector entities to build awareness and cooperative relationships to protect United States critical infrastructure and institutions.
- Conducting vulnerability assessments of both government and private sector entities to enable timely, effective countermeasures.
- Developing training policy and standards for CI and security professionals.

NCSC Organization

National Intelligence Manager for CI (NIM-CI)

The Director, NCSC, also serves as the NIM-CI, responsible for oversight and integration of CI activities across the IC. NIM-CI provides strategic guidance by means of a Unified Intelligence Strategy (UIS) for CI, a classified strategy that provides a framework for enabling CI program managers across the IC to align resources with prioritized requirements tied to programs directed at achieving particular strategic objectives. The NIM-CI also conducts mission reviews of CI programs and activities to assess their impact and alignment with national CI strategy.

National Insider Threat Task Force (NITTF)

One component of NCSC, the NITTF, which is chaired by the DNI and the Attorney General, was originally established through Executive Order 13587 in October 2011. The NITTF is responsible for developing policy and programs for deterring, detecting, and mitigating threats from personnel within the government or private industry who would unlawfully disclose classified information, or in any way work to undermine U.S. national security on behalf of a foreign entity. NCSC Director Evanina has underscored the seriousness of the continued risk posed by insider threat, noting that it remains "as much a problem today as … five years ago." The NITTF is also responsible for outreach to increase public awareness of the threat and provide best practices for deterrence, detection and mitigation. Some analysts have contended that the potential for insider threat-related activities has grown with the proliferation of social media platforms that can conceal communications though end-to-end encryption.

Center for Security Evaluation (CSE)

The CSE provides advice and support to the Department of State on security for the construction and operation of diplomatic facilities overseas, including security construction requirements, assessments and mitigation of CI and security vulnerabilities, and force protection.

NCSC Directorates

The Operations Coordination Directorate helps to coordinate offensive and cyber CI operations, providing strategic guidance and assessments of the effectiveness of these programs. The Technical and Cyber Directorate is responsible for oversight of IC agency technical and signal security countermeasures, and cyber CI and security. The Supply Chain Directorate identifies and analyzes risks to the supply chain, conducts outreach campaigns to increase awareness of threats to the supply chain, and publishes risk management best practices.

Security Executive Agent (SecEA) and the Special Security Directorate (SSD)

Personnel comprising the NCSC's SSD serve as the executive staff supporting the DNI's role as SecEA, responsible for the "development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information." SSD professionals also support the SecEA's role as a principal on the Suitability and Security Clearance Performance Accountability Council (PAC), which oversees implementation of policy to overhaul the security clearance process. SSD specifies policy for security clearance reciprocity among federal government agencies. SSD also manages *Scattered Castles*, the national repository for recording eligibility for access to Sensitive Compartmented Information (SCI), other controlled access programs, and IC element visit certifications.

Table 1. NCSC Components

- National Intelligence Manager for CI (NIM-CI)
- National Insider Threat Task Force (NITTF)
- Center for Security Evaluation
- Operations Coordination Directorate
- Technical & Cyber Directorate
- Supply Chain Directorate
- Special Security Directorate

Source: NCSC.

Threat Environment

NCSC has been principally concerned with four countries: Russia, China, Iran, and North Korea, which it assesses to be responsible for political and economic espionage, cyberattacks, and information operations targeting the United States. State and nonstate threats to the United States have specifically targeted organizations and infrastructure connected to the defense, manufacturing, energy, financial, public health and emergency services, transportation, and telecommunications sectors. NCSC's *Strategic Plan* also highlights the growing risk posed by threats operating in cyberspace that can use social media platforms to influence public opinion, or exploit "smart" devices linked through the *internet of things*.

Acknowledgement: This In Focus was originally co-authored with former CRS Intern Jackson K. Stuteville.

Michael E. DeVine, medevine@crs.loc.gov, 7-1126

IF11006