National Counterintelligence and Security Center

STRATEGIC PLAN | 2018–2022

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

A Message from the Director

William R. Evanina
Director, NCSC

I am pleased to present the National Counterintelligence and Security Center's (NCSC's) *Strategic Plan* for fiscal years 2018-2022. NCSC's mission is to lead and support the US Government's counterintelligence (CI) and security activities critical to protecting our nation; provide outreach to US private sector entities at risk of intelligence penetration; and issue public warnings regarding intelligence threats to the US. The Center's vision is to carry out its mission in a way that ensures it is the premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

The openness of America—our government, industries, universities and research labs in pursuit of scientific discovery and innovation—makes us a prime target of foreign intelligence entities. The technologies that connect people to computers and networks also provide a nexus for adversarial penetrations, theft of intellectual property and unauthorized disclosures through remote access and through the recruitment of insiders. As we face higher physical and technical threat levels than ever before, our security policies, standards, guidelines and practices must be based on sound threat analysis and risk management. US Government CI and security activities protect our nation's secrets and assets from theft, manipulation or destruction by foreign adversaries by knowing their intentions, targets, capabilities and methods. The overarching theme of our *Strategy* is the integration of CI and security activities because the solutions to countering adversarial threats often lie at the intersection of the CI and security disciplines.

While our five Strategic Goals are individually important, they cannot be executed in isolation. NCSC is uniquely positioned to integrate the tremendous assets of the CI, security and cyber communities and to achieve mission success through collaboration and partnerships. This *Strategy* defines our mission, vision, strategic goals, key objectives and initiatives that will guide our choices and direct our resources in how we will work with our mission partners and stakeholders to deter and defeat any adversary that threatens our national security.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. The targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.*

**Worldwide Threat Assessment of the US Intelligence Community 2017.*

Purpose of this Plan

NCSC activities must be consistent with and responsive to national security priorities and comply with the US Constitution, applicable statutes and Congressional oversight requirements. In fulfilling NCSC's responsibilities under the *National Security Act of 1947, Counterintelligence Enhancement Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),* Executive Orders, Intelligence Community Directives and in support of the *National Security Strategy*, the *National Intelligence Strategy* and the *National Counterintelligence Strategy of the United States of America,* this *Strategic Plan* provides our mission partners, stakeholders, and our workforce with our mission, vision, goals, objectives and key initiatives.

MISSION

Lead and support the US Government's counterintelligence and security activities critical to protecting our nation; provide counterintelligence outreach to US private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the US.

VISION

NCSC is the nation's premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

STRATEGIC GOALS

Goal 1:
Advance our Knowledge of, and our Ability to Counter Foreign and other Threats and Incidents.

Goal 2:
Protect US Critical Infrastructure, Technologies, Facilities, Classified Networks, Sensitive Information, and Personnel.

Goal 3:
Advance our Counterintelligence and Security Mission and Optimize Enterprise Capabilities through Partnerships.

Goal 4:
Strengthen our Effectiveness through Stakeholder Engagement, Governance, and Advocacy.

Goal 5:
Achieve our Mission through Organizational Excellence.

Contents

Foreign Intelligence Threats

As a backdrop for NCSC's *Strategic Plan*, this excerpt from the 2017 *Worldwide Threat Assessment*, succinctly summarizes the leading state and non-state intelligence threats to US interests, as well as their targets and methods. These threats underpin NCSC's Counterintelligence and Security misson and strategic goals.

Counterintelligence

The United States will face a complex global foreign intelligence threat environment in 2017. The leading state intelligence threats to US interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope. Other states in South Asia, the Near East, East Asia, and Latin America will pose local and regional intelligence threats to US interests.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. The targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Non-state entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities including by human, technical, and cyber means. As with state intelligence services, these non-state entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2017 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat. Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years.

Russia

Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure. Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture.

China

China will continue actively targeting the US Government, its allies, and US companies for cyber espionage. Private sector security experts continue to identify ongoing cyber activity from China. Beijing has also selectively used offensive cyber operations against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy.

Iran

Iran continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats—including against US allies in the region. Iran has also used its cyber capabilities directly against the United States.

North Korea

North Korea has previously conducted cyber-attacks against US commercial entities, and remains capable of launching disruptive or destructive cyber attacks to support its political objectives.

Counterintelligence, Security, and Cyber

Rapid technological advances are enabling a broad range of foreign intelligence entities[1] (FIEs) to refine their cyber capabilities and target the US Government, private sector, and academia. FIEs aggressively use cyber operations to advance their interests and gain advantage over the US. These activities intensify traditional FIE threats, place US critical infrastructure and technologies at risk, erode US competitive advantage, and weaken our global influence. In formulating this *Strategy* we note that cyber threats and attacks by FIEs are considered both a CI and security challenge.

Counterintelligence

Counterintelligence programs collect information and conduct activities 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.

Cyber Threats

Foreign Intelligence Entities conduct cyber operations to penetrate our public and private sectors in the pursuit of policy and military insights, sensitive research, intellectual property, trade secrets, and personally identifiable information (PII). FIE cyber activities present both CI and security threats.

Security

Security programs and activities establish personnel, physical, information, operational, industrial and technical safeguards and countermeasures to protect US Government information, critical infrastructure, networks, personnel, and facilities from all threats.

NCSC works with the Intelligence Community and US Government cyber community to provide the CI and security perspective on foreign adversarial cyber capabilities, intent, and attribution.

To mitigate FIE threats, the IC must drive innovative CI and security solutions, further integrate CI, security, and cyber disciplines into IC business practices, and effectively resource such efforts. While the authorities that govern CI and security and the programs they drive are distinct, their respective actions must be synchronized, coordinated, and integrated.

[1] A foreign intelligence entity (FIE) is any known or suspected foreign state or non-state organizations or persons that conducts intelligence activities to acquire US information, block or impair US intelligence collection, unlawfully influence US policy, or disrupt US systems and programs. The term includes foreign intelligence and security services and international terrorists. *Intelligence Community Directive* (ICD) 750.

A Counterintelligence and Security Perspective on the Threat Environment

Threat Actors

There are many more highly capable foreign intelligence services in the world than ever before. Threats to US national and economic security come from a range of malign actors including nation states with highly sophisticated intelligence services and cyber programs; nations with lesser technical capabilities but possibly more disruptive intent; ideologically motivated hackers, profit-motivated criminal enterprises, terrorist organizations, and insiders.

Threats from Foreign Intelligence Entities

The US faces persistent and substantial threats from the activities of FIEs. These adversaries relentlessly target the US Government; US critical infrastructure; national security information; proprietary information from US companies; and research institutions involved in defense, energy, finance, dual-use technology, and other sensitive areas.

Advancing our knowledge and understanding of FIE plans, intentions, capabilities, tradecraft and operations will enable us to strengthen America's protective barrier against their hostile intent and actions.

Threats from Insiders and Unauthorized Disclosures

The IC, US Government organizations and the private sector continue to face insider threats, data breaches, and unauthorized disclosures. When trusted insiders disclose sensitive US Government information to the public they degrade and disrupt our ability to conduct intelligence missions and provide our adversaries with a competitive advantage.

Anonymity and encryption tools, more users and devices, cloud computing, and advanced malware enable insiders to hide unauthorized actions among normal activities, and operate undetected to harvest valuable information. The unauthorized disclosure of classified information to the public via the media, whether for ideological or personal reasons, causes significant damage to national security. One action by one individual can cause disproportionate and enduring damage.

E3100A16C20Data BreachE204 65
12202E6F616368657320 4C697474
A7 01Cyber Attack696EA1 486F

Cyber Threats

America’s economy, safety, and health are linked through a networked infrastructure that is targeted by foreign governments, criminals, and individual actors who try to avoid attribution.

Cyber threats to classified and unclassified US information networks are increasing in frequency, scale, and severity of impact. The range of cyber threat actors, methods of attack, targeted systems and victims is also expanding. The information and communication technology (ICT) networks that support US Government, military, commercial and social media activities remain vulnerable to espionage, hacking and disruption.

The widespread incorporation of “smart” devices into everyday objects, often referred to as the “Internet of Things” (IoT) is changing how people and machines interact with each other and the world around them. Their deployment has also introduced vulnerabilities into the infrastructure that they support. For every American, this means that personally identifiable information (PII) can be stolen through hacks of companies, retailers, social media sites and US Government networks.

Cyber actors have already used these smart devices for distributed denial-of-service (DDoS) attacks, and they will continue. In the future, state and non-state actors will likely use IoT devices to support security or to access or attack targeted computer networks.[2]

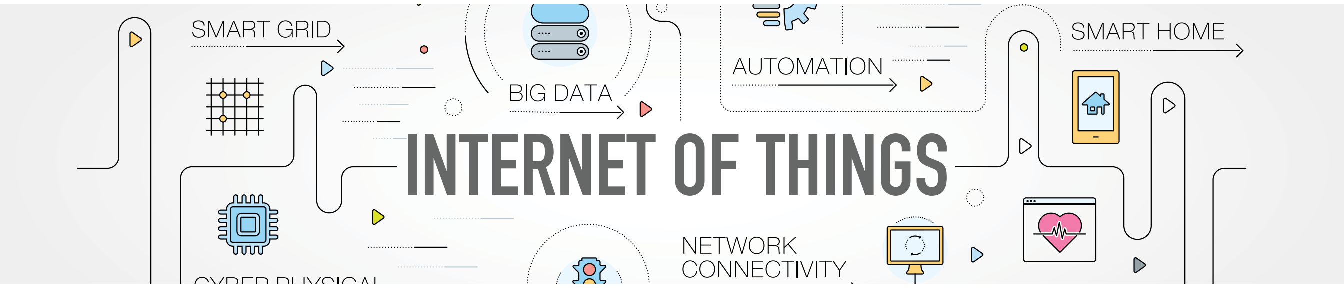
Physical Threats

US Government personnel and facilities, both domestic and abroad, are increasingly under threat of physical attack by hostile actors seeking to cause death and destruction. Physical security threats come from a variety of hostile actors including lone gunmen, domestic terrorists, and organized foreign terrorists. Other physical threats to our personnel and facilities come from those opposed to US Government policies and activities. While they may not commit violent acts, they aim to disrupt daily business. Such efforts may be in the form of demonstrations, blocking access to buildings, sabotaging equipment, or physically harassing workers.

Threats to the Supply Chain

The global nature of critical US supply chains increases the threat for subversion of our critical infrastructure, industrial and national security sectors. Attribution of FIE exploitation of supply chains is difficult due to the clandestine nature and methods of supply chain operations.

Securing US critical supply chains from FIE attempts to compromise the integrity, trustworthiness and authenticity of products and services purchased and integrated into the operations of the US Government and industry is an enduring CI and security challenge.



[2] *Worldwide Threat Assessment of the US Intelligence Community, May 2017.*

Threats to US Technologies and Intellectual Property

Scientific discovery and innovation empower America with a competitive edge that secures our military advantage and propels our economy. America's culture of openness and collaboration in science and technology makes our national labs, universities, private sector, high-value targets for economic espionage and theft of US intellectual property by foreign actors.

The foreign threat to US intellectual property is growing, whether measured by FBI investigations, criminal convictions, or the number and sophistication of cyber intrusions. Many state actors view economic espionage as essential in achieving their own national security and economic goals at the expense of ours. They employ commercial enterprises owned or influenced by the state, particularly when seeking sensitive technologies. Some nation-states direct their national intelligence services to steal intellectual property to provide competitive advantage to their own indigenous innovation goals. Understanding how some foreign governments mix business with espionage illustrates the blurred lines between traditional intelligence collection and economic espionage.

Threats to US Critical Infrastructure[3]

The counterintelligence efforts to protect US critical infrastructure are to detect, deter or disrupt any FIE attempts to launch disruptive operations against America's infrastructure.

The US Government and private sector firms alike are increasingly concerned about state and non-state sponsored attempts to control or debilitate critical infrastructure systems, corrupt supply chains, or to gain access to sensitive networks and information that control our nation's critical infrastructure.

The asymmetric, offensive opportunities available to FIEs from systemic and persistent vulnerabilities in key sectors of US infrastructure continue to grow. A foreign adversary gaining access to industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems that monitor and control plants or equipment in industries such as telecommunications, transportation or energy, could seriously disrupt or damage the US economy and national security.

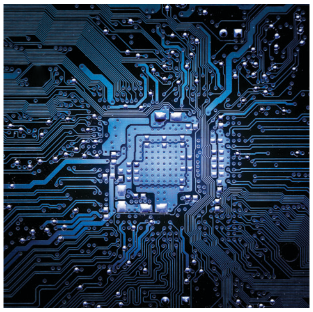
[3] Critical infrastructure represents systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters. (USA Patriot Act of 2001 § 1016(e)).

Sixteen Sectors of US Critical Infrastructure

Chemical

Dams

Financial Services


Information Technology

Commercial Facilities

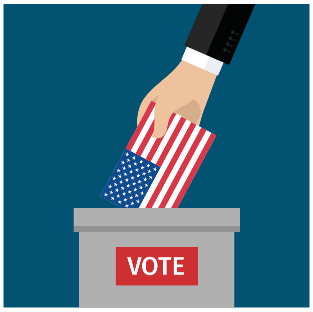
Defense
Industrial Base

Food and Agriculture

Nuclear Reactors,
Materials, and Waste

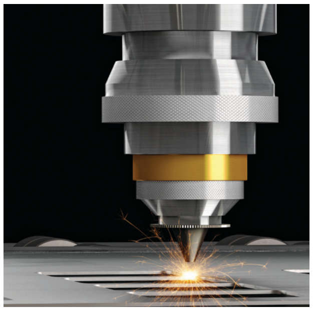
Communications

Emergency Services



Government Facilities[4]

Transportation Systems


Critical Manufacturing

Energy

Healthcare and
Public Health

Water and
Wastewater Systems

[4] In January 2017, the US election infrastructure was designated by the Department of Homeland Security as a subsector of the existing Government Facilities Sector.

The National Counterintelligence and Security Center: An Overview

NCSC's Counterintelligence Responsibilities for the US Government and the Intelligence Community

The Director of NCSC serves as National Intelligence Manager for Counterintelligence (NIM-CI) for the IC.

NCSC's National Role for Security

NCSC is responsible for producing, in consultation with US Government departments and agencies, the *National Threat Identification and Prioritization Assessment (NTIPA)*, a strategic assessment of FIE threats against the US; and the *National Counterintelligence Strategy of the United States of America (National CI Strategy)* to guide programs and activities that guard against foreign threats. NCSC, with its mission partners, drafts, monitors and evaluates the *National CI Strategy* implementation and submits an annual mission review report to the DNI, including a discussion of any shortfalls and recommendations for remedies. In its national role NCSC oversees and coordinates the production of national CI strategic analysis, including damage assessments from espionage and unauthorized disclosures, and lessons learned from these activities. NCSC also coordinates national CI collection and targeting; and develops priorities for CI investigations and operations.

NCSC's Intelligence Community Role for CI

The Director of NCSC, as the National Intelligence Manager for Counterintelligence (NIM-CI) is the DNI's principal substantive adviser on all aspects of CI. In this role, NIM-CI produces and updates the *Unifying Intelligence Strategy* (UIS)[5] for CI.

A team that includes a National Intelligence Officer for CI (NIO-CI)[6] on the National Intelligence Council (NIC)[7], a National Intelligence Collection Officer (NICO)[8], and National Counterintelligence Officers (NCIOs)[9] works collaboratively to identify opportunities to integrate collection, analysis and CI efforts to achieve unity of effort and effect, and advises the DNI, through NIM-CI, on the state of the CI mission.

[5] The *Unifying Intelligence Strategy* (UIS) is developed by NIM-CI to integrate the efforts of the IC. It is a coordinated strategic document that defines key focus areas/priorities, identifies gaps and develops initiatives to address these gaps. The UIS is disseminated to the IC, Congress and the National Security Council.

[6] NIO-CI leads CI strategic analysis in the IC and articulates substantive intelligence priorities to guide intelligence analysis and production.

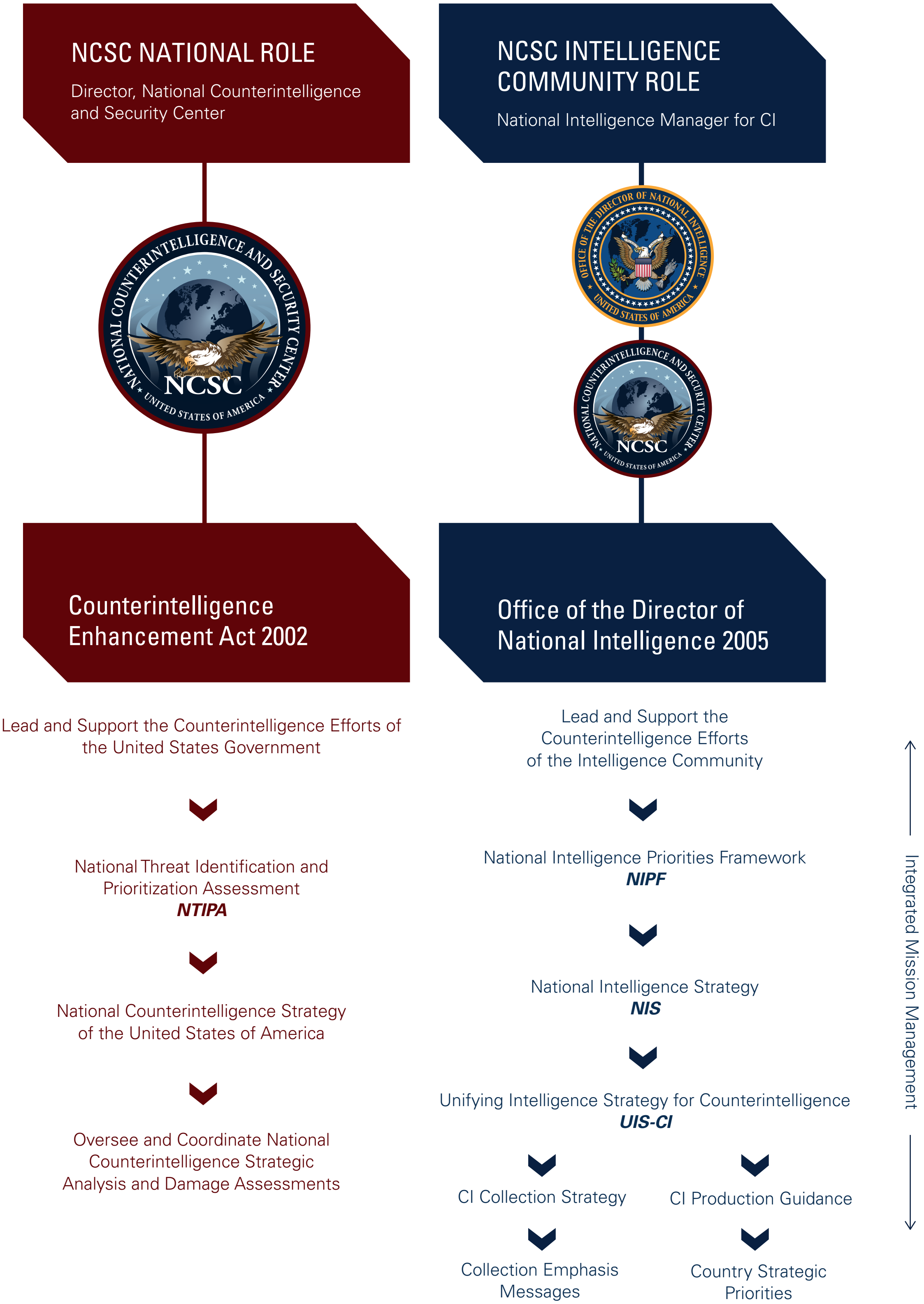
[7] The NIC consists of senior intelligence analysts supporting the DNI in carrying out responsibilities as head of the IC and as the principal adviser to the President and the National Security Council (NSC) for intelligence matters related to national security.

[8] NICO is the senior expert who serves as the principal collection advisor, leading strategic alignment and integration of collection resources for maximum mission impact. NICOs are responsible for integrating collection priorities and perspectives into mission management, UIS, and policy discussions where appropriate.

[9] NCIOs are the substantive CI experts on identifying, prioritizing and countering foreign intelligence threats. They inform policymakers, the DNI, NIM-CI, and regional NIMs on current and emerging CI issues within their respective areas of responsibility.

NCSC Counterintelligence Responsibilities

The Director of NCSC serves in a national and Intelligence Community capacity. The graphic below delineates NCSC's national and Intelligence Community role based on legislation, Executive Orders, Intelligence Community Directives and national strategic guidance.



NCSC NATIONAL ROLE

Director, National Counterintelligence and Security Center

Counterintelligence Enhancement Act 2002

Lead and Support the Counterintelligence Efforts of the United States Government

National Threat Identification and Prioritization Assessment
NTIPA

National Counterintelligence Strategy of the United States of America

Oversee and Coordinate National Counterintelligence Strategic Analysis and Damage Assessments

NCSC INTELLIGENCE COMMUNITY ROLE

National Intelligence Manager for CI

Office of the Director of National Intelligence 2005

Lead and Support the Counterintelligence Efforts of the Intelligence Community

National Intelligence Priorities Framework
NIPF

National Intelligence Strategy
NIS

Unifying Intelligence Strategy for Counterintelligence
UIS-CI

CI Collection Strategy

Collection Emphasis Messages

CI Production Guidance

Country Strategic Priorities

Integrated Mission Management

NCSC's Security Responsibilities for the US Government and the Intelligence Community

The DNI designated NCSC to be responsible for executing Security Executive Agent (SecEA) authorities across the Executive Branch, and to oversee and direct the protection and safeguarding programs across the Intelligence Community.[10]

NCSC's National Role for Security

The SecEA focuses on protecting our national security interests by ensuring the reliability and trustworthiness of those to whom we entrust our nation's secrets and assign to sensitive positions. In the national role of SecEA, the DNI, through NCSC, drives US Government-wide security clearance modernization efforts by developing an overarching strategy and tools; applying information technology to improve the timeliness and quality of investigative and adjudicative processes; while overseeing these processes to ensure their effectiveness.[11]

Protecting Sensitive Compartmented Information

NCSC, as designated by the DNI, oversees the protection of national security networks, information, facilities and personnel through a Defense-in-Depth methodology implemented uniformly across the Executive Branch agencies and industry. NCSC unifies the security activities of these entities under a common framework that is consistently implemented, critically assessed and improved through joint policy development.

To improve the security of classified networks and the responsible sharing and safeguarding of classified information across the Executive Branch, NCSC supports national strategic and tactical objectives through policy formulation, oversight and assessment of common objectives.[12]

NCSC's Intelligence Community Role for Security

NCSC provides and maintains a common security infrastructure that strengthens partnerships across the IC, enhances access controls to facilities and technology and enables fluid responses in times of national crises and mobilization.

NCSC leads an IC research and analysis partnership devoted to the development, identification, and integration of physical and technical capabilities to mitigate adversary exploitation of potential vulnerabilities. These research and analysis activities evaluate technical security shortfalls, identify solutions, and manage the integration of emerging technologies to improve security countermeasures.

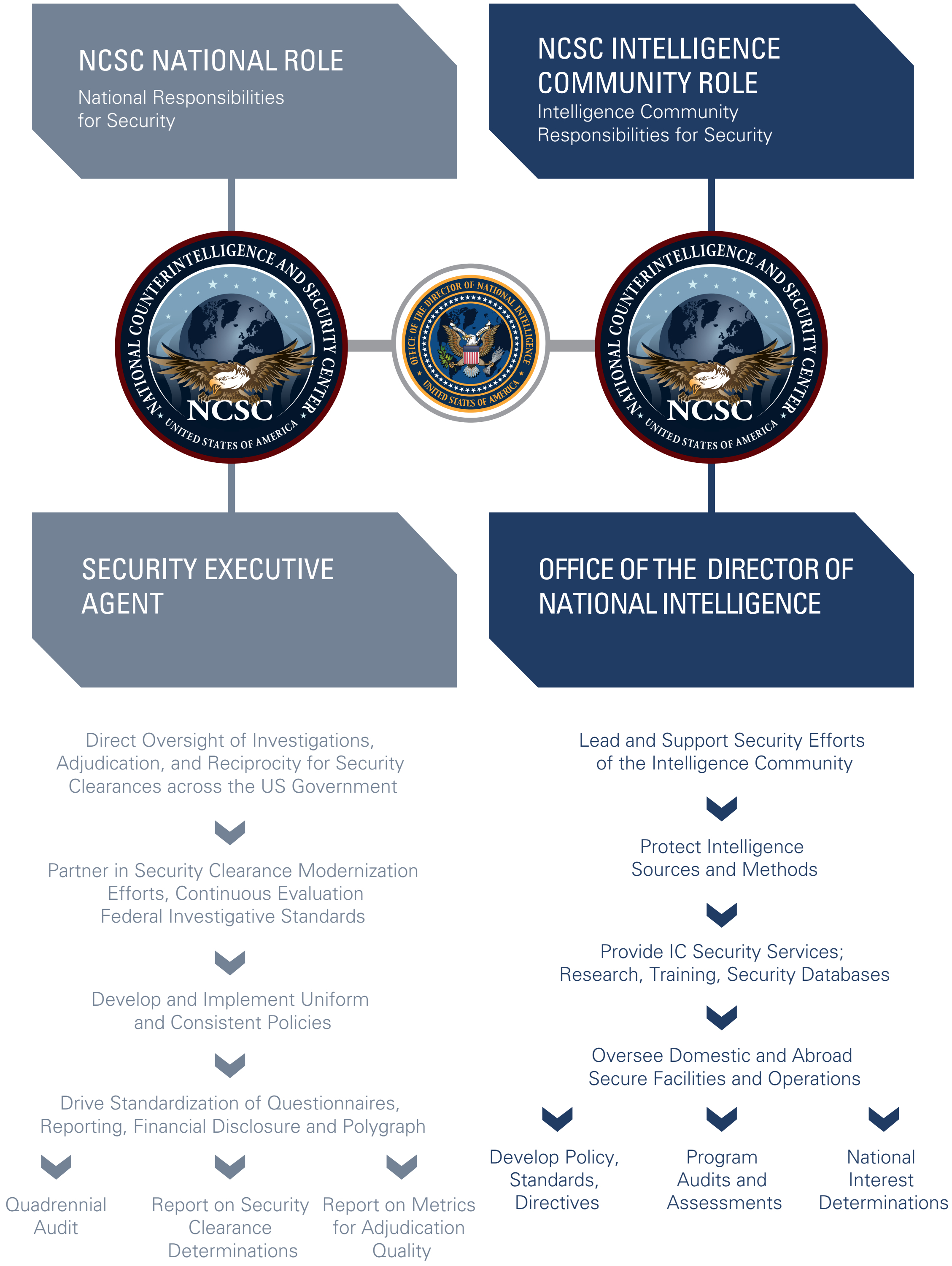
[10] Executive Order 13467 affirmed the DNI as SecEA to oversee Executive Branch investigations and determination activities, and to serve as final authority to designate an authorized investigative or adjudicative agency.

[11] The Intelligence Reform and Terrorism Prevention Act (IRTPA) provides that a single department, agency, or element shall be responsible for various functions relating to personnel investigations and adjudications.

[12] Executive Order 13587. *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.*

NCSC Security Responsibilities

For security, NCSC is responsible for Security Executive Agent activities across the Executive Branch and is the DNI's designee for oversight and direction for safeguarding national security programs across the IC. The graphic below delineates these responsibilities based on legislation, Executive Orders, Intelligence Community Directives, Executive Correspondence and national policy guidance.



NCSC NATIONAL ROLE

National Responsibilities for Security

NCSC INTELLIGENCE COMMUNITY ROLE

Intelligence Community Responsibilities for Security

SECURITY EXECUTIVE AGENT

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Direct Oversight of Investigations, Adjudication, and Reciprocity for Security Clearances across the US Government

Partner in Security Clearance Modernization Efforts, Continuous Evaluation Federal Investigative Standards

Develop and Implement Uniform and Consistent Policies

Drive Standardization of Questionnaires, Reporting, Financial Disclosure and Polygraph

Quadrennial Audit

Report on Security Clearance Determinations

Report on Metrics for Adjudication Quality

Lead and Support Security Efforts of the Intelligence Community

Protect Intelligence Sources and Methods

Provide IC Security Services; Research, Training, Security Databases

Oversee Domestic and Abroad Secure Facilities and Operations

Develop Policy, Standards, Directives

Program Audits and Assessments

National Interest Determinations

NCSC Mission Partners and Stakeholders

IC mission partners, our Federal Partners, including those responsible for protecting sectors of US critical infrastructure, and our stakeholders, play a vital role in assisting NCSC to advance the CI and security mission and optimize enterprise capabilities. While our mission partners and stakeholders are not mutually exclusive, we highlight the importance of both in this *Strategy*, and distinguish between them in the following way.

NCSC Mission Partners | *Collaborate for Mission Success*

NCSC mission partners are those organizations and disciplines that help advance, contribute to, or execute CI and security missions. They can be US Government, Intelligence Community and our allied foreign partners. Mission-enabling disciplines that support or are supported by CI and security activities include legal, acquisition, information technology, information assurance, and civil liberties, privacy, and transparency.

NCSC Stakeholders | *Advocate for CI and Security*

Our stakeholders are linked to NCSC by governance, oversight and resources. They are CI and security representatives from the US Government and the Intelligence Community. They are advocates within their own organizations and agents of change for implementing national CI and security strategies. NCSC advocates for stakeholders funded by the National Intelligence Program (NIP) for resources, policies and programs, and to Congress on behalf of our Federal Partners for CI and security programs. Our Congressional oversight committees, the National Security Council, the White House and through these institutions, ultimately, the American people, are significant stakeholders in all that we do.

NCSC Federal Partners*

Department of State

Department of the Treasury

Department of Defense

Department of Justice

Department of the Interior

Department of Agriculture

Department of Commerce

Department of Labor

Department of Housing and Urban Development

Department of Health and Human Services

Department of Transportation

Department of Energy

Department of Education

Department of Veterans Affairs

Department of Homeland Security

*We also include independent commissions and agencies and their contractors.

An Overview of NCSC Responsibilities

Threat Assessments to Disrupt and Defeat the Adversary

The foundation of all counterintelligence work is to build in-depth knowledge of FIE intentions, targets, and capabilities, in order to mitigate threats posed by these entities.

NCSC produces the *National Threat Identification and Prioritization Assessment (NTIPA)* which informs policymakers and senior officials with CI responsibilities on current and emerging foreign intelligence threats that could seriously damage US national security.

The National Intelligence Priorities Framework (NIPF) reflects policymakers' priorities for national intelligence support and ensures that enduring and emerging intelligence issues are addressed. NCSC is the CI Topic Manager for the NIPF. The NCSC Director, in the role of NIM-CI provides coordination with our NIO for CI at the NIC, in planning and producing timely, accurate and insightful CI strategic[13] and anticipatory[14] intelligence derived from planned collection on the activities directed against the US by foreign powers, their intelligence services or their proxies. This intelligence informs coordinated offensive and defensive CI activities to effectively counter, disrupt and defeat FIE attempts to undermine US national interests.

Personnel Security

For personnel security, NCSC serves in support of the DNI's role as SecEA. SecEA authorities direct the SecEA to develop, implement, oversee and integrate joint security and suitability initiatives with its US Government partners for effective, efficient, and uniform policies and procedures in conducting investigations and adjudications for eligibility for access to classified information or to hold a sensitive position.

Continuous Evaluation (CE) is a personnel security investigative process that leverages an automated records check methodology and applies standardized business rules to identify adjudicatively relevant information to assess cleared individuals' ongoing eligibility for access to classified information. CE supplements the periodic reinvestigation security clearance process.

CE programs are designed to manage risk through warning and preemptive intervention; minimize information gaps between security clearance reinvestigations; develop policy and guidance and provide oversight of CE programs. NCSC develops policies, standards, and guidance for establishing CE programs for the IC and for our Federal Partners, and then coordinates, aligns, and integrates their CE activities.

[13] Strategic intelligence is the process and product of developing the context, knowledge and understanding of the strategic environment required to support US national security policy and planning decisions. This work includes identifying and assessing the capabilities, activities, and intentions of state and non-state entities to identify risks to and opportunities for US national security interests. *National Intelligence Strategy 2014.*

[14] Anticipatory intelligence involves collecting and analyzing information to identify new, emerging trends, changing conditions, potential trends and undervalued developments, which challenge long-standing assumptions, encourage new perspectives, as well as provide warning of new opportunities and threats to US interests. *National Intelligence Strategy of the United States of America, 2017. National Intelligence Strategy 2014.*

The National Insider Threat Task Force [15]

NCSC co-leads, with the FBI, the National Insider Threat Task Force (NITTF). The NITTF helps the Executive Branch build programs that deter, detect and mitigate actions by insiders who may represent a threat to national security. The NITTF develops guidance, provides assistance, assesses progress and analyzes new and continuing insider threat challenges. It is important to note that insider threat programs target anomalous activities, not individuals, so the NITTF's work is coordinated with the relevant organization's records management office, legal counsel, and civil liberties and privacy officials to build-in protections against infringing upon employees' civil liberties, civil rights, privacy and whistleblower protections.

Information Sharing and Audit Data

IC elements treat information collected and analysis produced as national assets and are stewards of information who have a "responsibility to provide." Authorized IC personnel have a "responsibility to discover" information believed to contribute to their assigned mission need and a corresponding "responsibility to request" information they have discovered. The discovery, retrieval and dissemination of information within the IC requires making all national intelligence available for discovery by automated means—and therein lies the vulnerability. NCSC works in consultation with the IC Chief Information Officer (IC CIO) to develop IC enterprise standards for audit events to support information sharing, insider threat detection, and implementation of these standards.

Damage Assessments

NCSC leads and coordinates damage assessments, as directed by the DNI. IC damage assessments evaluate actual or potential damage to national security from the unauthorized disclosure or compromise of classified information. Lessons learned from these assessments are shared with our mission partners to improve CI and security programs and develop mitigation measures.

Physical Security
Protecting Facilities Domestically and Abroad

NCSC oversees the management of US Government facilities containing Sensitive Compartmented Information Facilities (SCIFs), and maintains a framework for common security standards for IC domestic facilities enabling savings through shared, multi-use spaces.

NCSC provides a single automated source for secure facility information worldwide. The tool can be invaluable for identifying SCIF locations in jeopardy due to national disasters, heightened security alerts, as well as domestic and international hostilities.

[15] Executive Order 13587 established the Insider Threat Task Force to develop Government-wide program for deterring, detecting, and mitigating insider threats. The Task Force is co-chaired by the Attorney General and the Director of National Intelligence, or their designees. It is staffed by personnel from the FBI and NCSC. To the extent permitted by law, NCSC provides an appropriate work site and administrative support for the Task Force.

Protecting US Embassies and Consulates

NCSC, in consultation with the IC, works with Department of State (DoS) to protect classified national security information and to perform other security-related functions affecting US diplomatic and consular facilities abroad.

NCSC maintains databases on foreign intelligence threats to, and the vulnerabilities of US diplomatic facilities; collaborates with the IC and DoS to enhance information assurance standards and policies to protect classified national security information held in US diplomatic facilities; partners with DoS, industry and the IC to assess technical security shortfalls, identify solutions and manage the integration of emerging technologies to improve security countermeasures.

As the demand for wireless (WiFi) devices and networks in IC work spaces and in US diplomatic facilities increases, NCSC leads the IC in developing new architectural shielding materials through a program that researches and advances new technologies to address emerging technical threats.

Technical and Signals Security Countermeasures

Disruptive technology is being built and fielded at an unprecedented rate. Countering the growing complexity of technological advances, both in the tools and methods used to employ them, requires greater technical literacy and a more comprehensive defensive countermeasures program.

Current technical and signals countermeasures and mitigation strategies are based upon Technical Surveillance Countermeasures (TSCM) and TEMPEST (emanations security) programs. TSCM programs detect, identify, and neutralize technical surveillance threats against facilities and their occupants.

TEMPEST refers to investigating, studying, and controlling compromising, unencrypted emanations from IT systems and equipment that can reveal sensitive information.

The TSCM community is aligned with and governed by the CI and security community, while the TEMPEST community is aligned with and governed by the Information Assurance (IA) community.

To better posture the IC to meet the challenges of rapidly advancing foreign technical threats and to close the current gaps in our defenses, NCSC leads a community-wide initiative to modernize and integrate the TEMPEST and TSCM communities under a uniformly defined Technical and Signals Security Countermeasures (TSSC) mission structure within the broader IC and intelligence cycle.

Supply Chain Risk Management

NCSC leads its mission partners in assessing and mitigating the activities of FIE and any other adversarial attempts aimed at compromising the global network of pathways—supply chains that provide mission-critical products, materials and services to the US Government. Supply chain risk management (SCRM) requires that subject matter experts in acquisition, CI, security, information assurance, logistics, and analysis, work in a common collaborative environment to share threat assessments, vulnerability and mitigation information. NCSC works closely with the acquisition and CIO communities to identify and advise of significant threats to US Government supply chains, including those associated with contractors and vendors.

Cyber Threats and Counterintelligence

The cyber threat is simultaneously a national security threat and a counterintelligence problem. State and nonstate actors use cyber operations to achieve economic and military advantage, foment instability, increase control over content in cyberspace and achieve other strategic goals. NCSC works with the US Government cyber community and the IC, to provide the CI and security perspective on FIE and other threat actors' cyber capabilities for context and possible attribution of adversarial cyber activities.

In partnership with the IC-CIO, NCSC participates in the integrated defense of the IC Information Environment through the IC Security Coordination Center (IC SCC). The IC SCC facilitates accelerated detection and mitigation of cyber threats across the IC by providing end-to-end security, situational awareness, and incident case management. It maintains consolidated insight into IC networks and intelligence information systems and coordinates IC responses to cyber events, incidents, outages, threats and technical vulnerabilities.

National and Intelligence Community Policy and Strategy Development

Policy Development

NCSC is responsible for national CI and security policy development, compliance and oversight. The National Counterintelligence Policy Board, chaired by the Director of NCSC, serves as the principal mechanism for developing national policies and setting priorities guide the conduct of CI activities across the US Government.

For personnel security under SecEA authorities, in coordination with the Suitability Executive Agent, NCSC ensures that policies, procedures and standards relating to suitability of contractor and employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information are aligned to the extent possible, for reciprocal recognition and protection of national security information.

NCSC facilitates and monitors the implementation and effectiveness of IC CI and security policies and programs, develops recommendations for new or modified policies; and develops and promulgates IC CI and security standards and other guidance to implement CI and security policies.

Strategy Development

NCSC leads the development, implementation and assessment of the *National Counterintelligence Strategy of the United States of America* to guide the US Government CI efforts. For the Intelligence Community, NCSC leads the development, implementation and assessment of the *Unifying Intelligence Strategy for Counterintelligence* and *Counterintelligence Strategic Priorities* along with comprehensive assessment programs to identify gaps, recommend priorities, and inform and shape resource and budget decisions.

Advocating for CI and Security Resources

The IC uses the Intelligence Planning Programming, Budgeting, and Evaluation (IPPBE)[16] system to effectively shape and sustain intelligence capabilities through the development of the National Intelligence Program (NIP). NCSC oversees the CI and security NIP resources and advocates for our Federal Partners to implement CI and security programs not funded by the NIP.

Transparency in budget planning and execution ensures that CI and security programs deliver the most effective results and reduce, restructure or terminate those programs that are not performing or have run their course. Through mission reviews, based on the implementation of the *National CI Strategy*, NCSC assesses progress toward closing key intelligence gaps and finds ways to leverage existing CI capabilities before proposing new ones. NCSC also advocates for security programs to include National Insider Threat and Continuous Evaluation Programs and for implementing Federal Investigative Standards.

Through various governance boards, NCSC also provides guidance to IC elements on developing budgets and spend plans associated with CI and security activities.

Civil Liberties, Privacy, and Transparency

NCSC safeguards privacy and civil liberties, and practices appropriate transparency in all CI and security programs to be accountable to ourselves and to the American people.

[16] The IPPBE system ensures a predictable, transparent and repeatable end-to-end process to collect and prioritize intelligence for mission requirements in the context of the strategic objectives of the DNI and the IC.

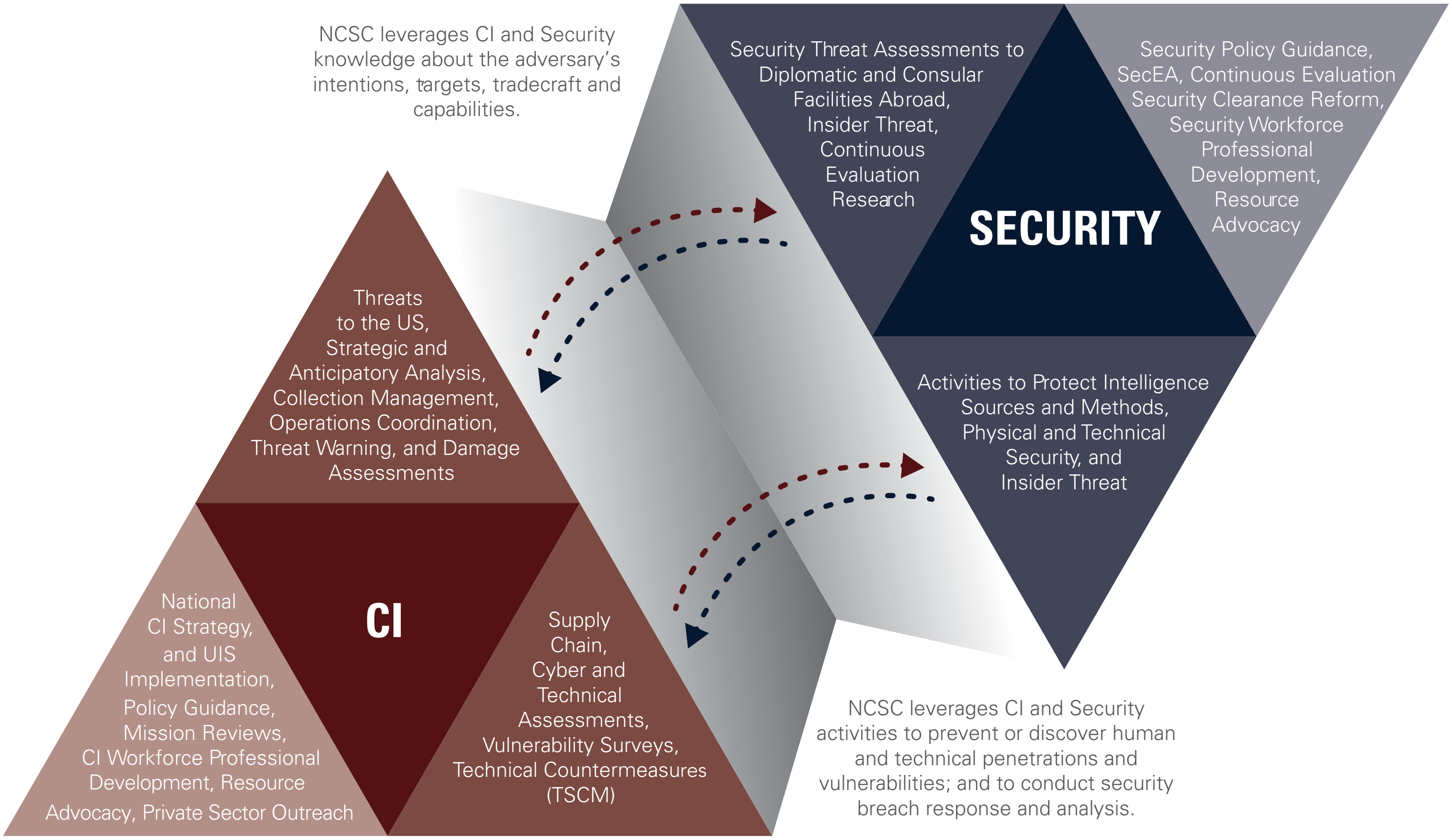
How NCSC Integrates Counterintelligence and Security Capabilities

COUNTERINTELLIGENCE

Includes all activities necessary to understand and defeat threats from malign actors. CI activities are grouped into three primary areas: **1)** Analysis, Collection, and CI Operations; **2)** Supply Chain, Cyber and Technical Threat and Vulnerability Assessments and Countermeasures; **3)** National CI Policy and Strategy, Performance Measurement, CI Workforce Professional Development Programs and Resource Advocacy

SECURITY

Includes all activities necessary to protect US critical infrastructure, classified networks, information and personnel. Security activities aregrouped into three primary areas: **1)** Security threat assessments; **2)** Measures and activities to protect sources and methods, security surveys and inspections; **3)** Policy Guidance, SecEA activities, Security Clearance Reform, Continuous Evaluation, Insider Threat Programs, Security Workforce Professional Development Programs and Resource Advocacy



NCSC leverages CI and Security knowledge about the adversary's intentions, targets, tradecraft and capabilities.

Security Threat Assessments to Diplomatic and Consular Facilities Abroad, Insider Threat, Continuous Evaluation Research

SECURITY

Security Policy Guidance, SecEA, Continuous Evaluation Security Clearance Reform, Security Workforce Professional Development, Resource Advocacy

Threats to the US, Strategic and Anticipatory Analysis, Collection Management, Operations Coordination, Threat Warning, and Damage Assessments

Activities to Protect Intelligence Sources and Methods, Physical and Technical Security, and Insider Threat

CI

National CI Strategy, and UIS Implementation, Policy Guidance, Mission Reviews, CI Workforce Professional Development, Resource Advocacy, Private Sector Outreach

Supply Chain, Cyber and Technical Assessments, Vulnerability Surveys, Technical Countermeasures (TSCM)

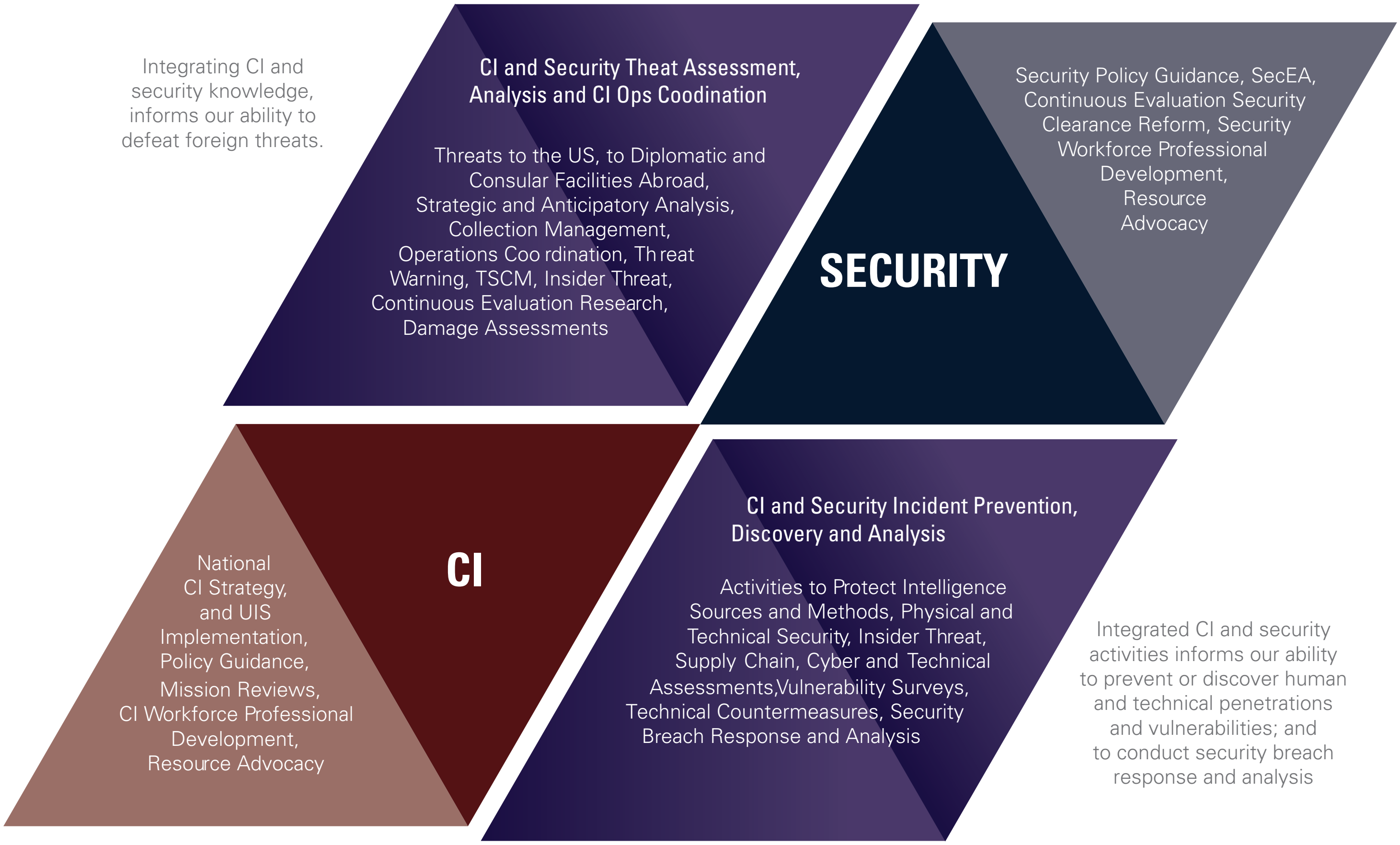
NCSC leverages CI and Security activities to prevent or discover human and technical penetrations and vulnerabilities; and to conduct security breach response and analysis.

NCSC Operating Principles

1 Leverage CI and security expertise to protect America against foreign and other threats.

2 Develop excellence in both CI and security disciplines.

NCSC blends CI and security expertise to lead and support the US Government's counterintelligence and security activities critical to protecting our nation; provide counterintelligence outreach to US private sectors entities at risk of foreign intelligence penetration; and issue public warning regarding intelligence threats to the US.



Integrating CI and security knowledge, informs our ability to defeat foreign threats.

CI and Security Theat Assessment, Analysis and CI Ops Coodination

Threats to the US, to Diplomatic and Consular Facilities Abroad, Strategic and Anticipatory Analysis, Collection Management, Operations Coordination, Threat Warning, TSCM, Insider Threat, Continuous Evaluation Research, Damage Assessments

SECURITY

Security Policy Guidance, SecEA, Continuous Evaluation Security Clearance Reform, Security Workforce Professional Development, Resource Advocacy

CI

National CI Strategy, and UIS Implementation, Policy Guidance, Mission Reviews, CI Workforce Professional Development, Resource Advocacy

CI and Security Incident Prevention, Discovery and Analysis

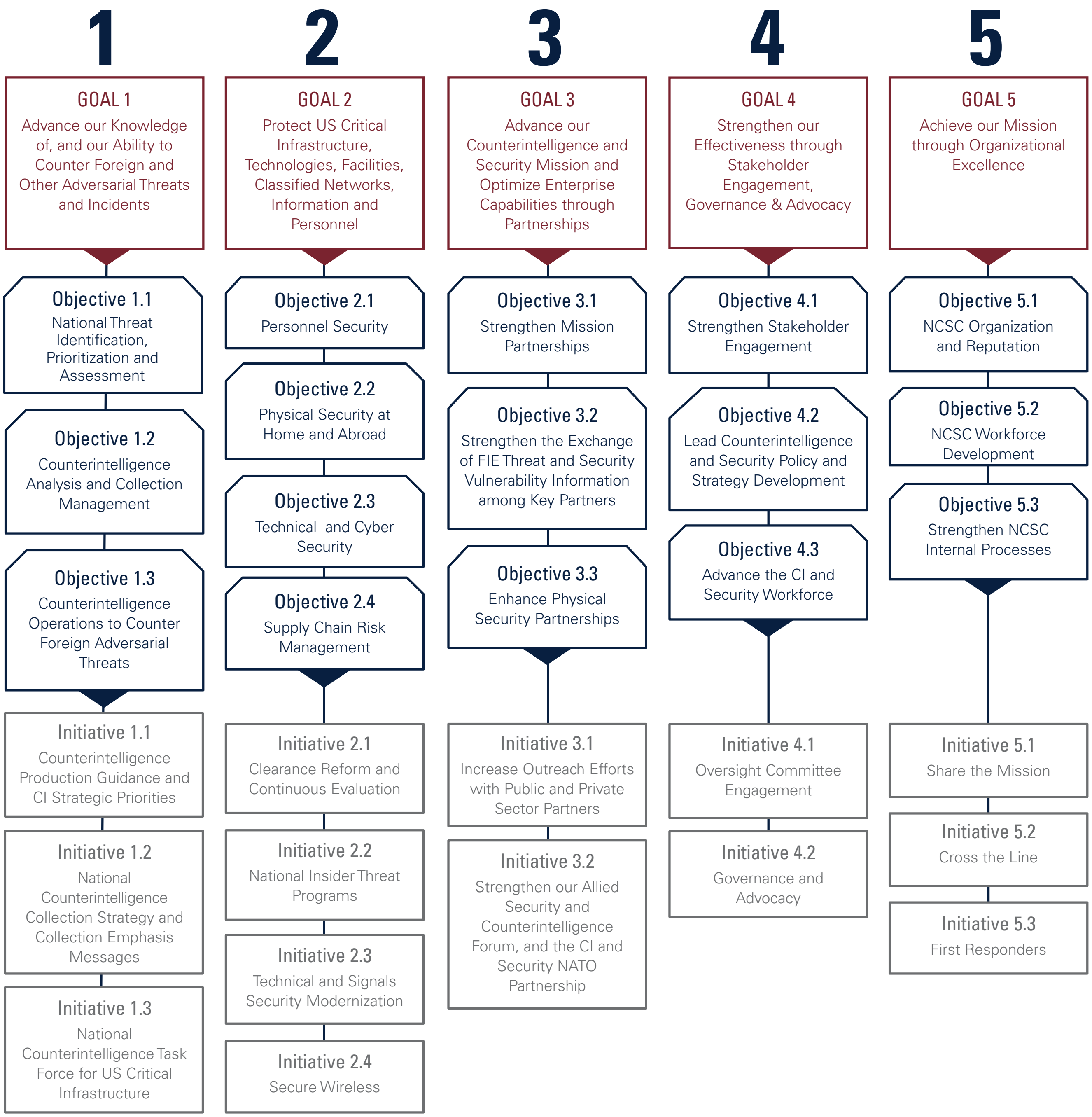
Activities to Protect Intelligence Sources and Methods, Physical and Technical Security, Insider Threat, Supply Chain, Cyber and Technical Assessments,Vulnerability Surveys, Technical Countermeasures, Security Breach Response and Analysis

Integrated CI and security activities informs our ability to prevent or discover human and technical penetrations and vulnerabilities; and to conduct security breach response and analysis

NCSC Strategic Goals, Objectives, and Initiatives

Our five *Strategic Goals* broadly describe how NCSC will integrate CI and security activities to address the enduring and emerging foreign and other adversarial threats. Our *Strategic Objectives* further define the work that must be done to achieve our goals. Initiatives can take many forms such as programs, projects, tools, systems or services. *Key Initiatives* outlined in this plan represent both new and continuing priorities.

NCSC Plan-at-a-Glance



1

GOAL 1
Advance our Knowledge of, and our Ability to Counter Foreign and Other Adversarial Threats and Incidents

Objective 1.1
National Threat Identification, Prioritization and Assessment

Objective 1.2
Counterintelligence Analysis and Collection Management

Objective 1.3
Counterintelligence Operations to Counter Foreign Adversarial Threats

Initiative 1.1
Counterintelligence Production Guidance and CI Strategic Priorities

Initiative 1.2
National Counterintelligence Collection Strategy and Collection Emphasis Messages

Initiative 1.3
National Counterintelligence Task Force for US Critical Infrastructure

2

GOAL 2
Protect US Critical Infrastructure, Technologies, Facilities, Classified Networks, Information and Personnel

Objective 2.1
Personnel Security

Objective 2.2
Physical Security at Home and Abroad

Objective 2.3
Technical and Cyber Security

Objective 2.4
Supply Chain Risk Management

Initiative 2.1
Clearance Reform and Continuous Evaluation

Initiative 2.2
National Insider Threat Programs

Initiative 2.3
Technical and Signals Security Modernization

Initiative 2.4
Secure Wireless

3

GOAL 3
Advance our Counterintelligence and Security Mission and Optimize Enterprise Capabilities through Partnerships

Objective 3.1
Strengthen Mission Partnerships

Objective 3.2
Strengthen the Exchange of FIE Threat and Security Vulnerability Information among Key Partners

Objective 3.3
Enhance Physical Security Partnerships

Initiative 3.1
Increase Outreach Efforts with Public and Private Sector Partners

Initiative 3.2
Strengthen our Allied Security and Counterintelligence Forum, and the CI and Security NATO Partnership

4

GOAL 4
Strengthen our Effectiveness through Stakeholder Engagement, Governance & Advocacy

Objective 4.1
Strengthen Stakeholder Engagement

Objective 4.2
Lead Counterintelligence and Security Policy and Strategy Development

Objective 4.3
Advance the CI and Security Workforce

Initiative 4.1
Oversight Committee Engagement

Initiative 4.2
Governance and Advocacy

5

GOAL 5
Achieve our Mission through Organizational Excellence

Objective 5.1
NCSC Organization and Reputation

Objective 5.2
NCSC Workforce Development

Objective 5.3
Strengthen NCSC Internal Processes

Initiative 5.1
Share the Mission

Initiative 5.2
Cross the Line

Initiative 5.3
First Responders

1 Goal 1: Advance our Knowledge of, and our Ability to Counter, Foreign and Other Threats and Incidents

With our mission partners, NCSC will lead the US Government and Intelligence Community efforts to identify, assess and mitigate threats and incidents from foreign and other adversaries that compromise our national security. National threat identification and prioritization; CI collection; strategic and anticipatory analysis; critical assessments of adversarial plans, intentions, targets, capabilities, tradecraft and operations; will advance our knowledge of and our ability to counter these threats, provide threat warning, and deliver analytic insights to US Government policymakers. To achieve this goal, NCSC has identified three strategic objectives and three initiatives:

Strategic Objectives

Objective 1.1 | National Threat Identification, Prioritization, and Assessment

Lead US Government efforts to identify, understand and prioritize threats from foreign intelligence entities and other adversaries that seek to harm US economic and national security.

Objective 1.2 | Counterintelligence Analysis and Collection Management

Drive analytic priorities for the CI community, assess the state of CI analysis and responsiveness to national priorities, and lead collaborative analytic initiatives to address high priority gaps. Manage CI collection requirements to assist in analysis, investigations and operations for critical CI and security missions.

Objective 1.3 | Counterintelligence Operations to Counter Foreign Adversarial Threats

Coordinate the activities conducted by our mission partners to anticipate, detect, disrupt and counter increasingly sophisticated adversarial capabilities and activities.

Initiatives

Initiative 1.1 | Counterintelligence Production Guidance and Strategic CI Priorities

Lead CI analytic community. Publish the annual *Counterintelligence Production Guidance*, and *Strategic Counterintelligence Priorities* to ensure IC assessments characterize the intentions, capabilities and targets of threat actors, identify intelligence gaps and impediments to closing them.

Initiative 1.2 | National Counterintelligence Collection Strategy and Collection Emphasis Messages

Lead the review, development, and enhancement of CI collection requirements to advance analysis, investigations and operations for CI and security missions.

Initiative 1.3 | National Counterintelligence Task Force for US Critical Infrastructure

Lead CI efforts to identify, anticipate, mitigate, and counter foreign intelligence threats to US critical infrastructure and sensitive US national security command, control, and communications infrastructure.

2 Goal 2: Protect US Critical Infrastructure, Technologies, Facilities, Classified Networks, Information, and Personnel

Blended operations by malign actors using human, technical, and cyber capabilities for data collection and exploitation, insider recruitment, and remote hacking into US classified information networks, signal the need for CI and security to build a more comprehensive understanding of foreign intelligence operations targeted against the US. CI and security programs must detect, deter and mitigate adversarial and insider threats. They must protect facilities, sectors of the US critical infrastructure, classified networks and information; identify and counter technical and cyber threats; and safeguard against malicious targeting of US supply chains. To achieve this goal, NCSC has identified four strategic objectives and four initiatives:

Strategic Objectives

Objective 2.1 | Personnel Security

Lead personnel security efforts for the Executive Branch. Develop and issue uniform and consistent policies, standards, and guidelines to ensure the effective, efficient, timely and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position. Direct oversight to ensure the consistent, effective, and timely implementation across the Executive Branch.

Objective 2.2 | Physical Security at Home and Abroad

Lead the physical security efforts to protect IC facilities domestically and abroad. Maintain a common framework using existing federal security standards to plan, design, protect and mitigate security risks. Consult and coordinate with the Department of State on physical security for diplomatic facilities where classified information is held and classified activities are conducted.

Objective 2.3 | Technical and Cyber Security

Lead our mission partners in identifying foreign technical penetrations, technical surveillance, or technical collection efforts against the US. Coordinate strategic analysis of technical and cyber threats; support vulnerability assessments; support CI operations.

Objective 2.4 | Supply Chain Risk Management

Investigate the threats to and vulnerabilities of US supply chains; engage our mission partners to neutralize and/or mitigate adversarial attempts to exploit US supply chain and acquisition vulnerabilities.

Initiatives

Initiative 2.1 | Clearance Modernization and Continuous Evaluation

Lead the Security Executive Agent (SecEA's) program to set investigative standards, and monitor implementation. Lead the Continuous Evaluation effort to enhance personnel security across the IC and the Executive Branch.

Initiative 2.2 | National Insider Threat Programs

Build National Insider Threat Programs so that Executive Branch Departments and Agencies with access to classified networks can deter, detect, and mitigate insider threats.

Initiative 2.3 | Technical and Signals Security Modernization

Lead an IC-wide initiative to modernize and integrate the TEMPEST and TSCM communities under a uniformly defined Technical and Signals Security Countermeasures mission structure.

Initiative 2.4 | Secure Wireless

Lead the CI and security efforts to identify wireless vulnerabilities and adversarial capabilities to exploit classified wireless networks.

3 Goal 3: Advance our Counterintelligence and Security Mission and Optimize Enterprise Capabilities through Partnerships

Partnerships are fundamental to our national security and that of our allies. Partners* offer access, expertise, capabilities and perspectives that enrich our intelligence capacity and help all of us succeed in our shared CI and security mission. Our approach to strengthening partnerships will be through initiatives that deepen our mutual understanding of CI and security challenges while ensuring the protection of sources, methods, activities, individual privacy and civil liberties. To achieve this goal, NCSC has identified three strategic objectives and two initiatives:

Strategic Objectives

Objective 3.1 | Strengthen Mission Partnerships

Establish new and strengthen existing mission partnerships to enhance our capacity to address CI and security challenges, promote the exchange of information, experiences, best practices and expertise, and facilitate consultation, collaboration and coordination for joint and cooperative CI and security activities.

Objective 3.2 | Strengthen the Exchange of FIE Threat and Security Vulnerability Information among Key Partners

Integrate the work of the CI operational, analytic, and security communities to counter, through the exchange of information, our adversaries' efforts to undermine US national interests.

Objective 3.3 | Enhance Physical Security Partnerships

Strengthen physical security capabilities through engagement with facilities mission partners to develop next generation smart construction technologies for facilities both domestic and abroad and ensure secure access to resupply.

Initiatives

Initiative 3.1 | Increase Outreach Efforts with Public and Private Sector Partners

Strengthen the exchange of FIE threat and security vulnerability information among key partners to promote coordinated approaches to mitigation, and advance the effectiveness of CI and security missions.

Initiative 3.2 | Strengthen our Allied Security and Counterintelligence Forum, and our CI and Security NATO Partnership

Strengthen our partnership and the exchange of information with our Allied Security and Counterintelligence Forum; enhance our CI and security partnership to affirm our CI and security support to NATO.

*Partners consist of organizations and entities working with us to advance national security priorities, including US military, our allies, foreign intelligence and security services; other federal departments and IC elements; as well as state, local and tribal governments and private sector entities. *National Intelligence Strategy of the United States of America 2017.*

4 Goal 4: Strengthen our Effectiveness through Stakeholder Engagement, Governance and Advocacy

Stakeholder engagement is central to our success. NCSC stakeholders play important roles as advocates, sponsors, partners and agents of change within their own organizations. Leading the CI and security communities requires shared governance, policy and strategy guidance, workforce professional development programs and resource advocacy. Through the *National CI Strategy* NCSC provides guidance for national-level CI programs; ensures that our mission partners address the enduring and emerging foreign intelligence threats; and that CI policies and programs are implemented and routinely evaluated for effectiveness and for continuous improvement. *The Unifying Intelligence Strategy for CI* guides CI collection and analytic efforts and influences future program and capability development. NCSC advocates for investment resources for CI and security programs and monitors the effectiveness of these programs across the US Government. NCSC keeps the Congressional intelligence oversight committees informed on all significant CI and security activities. To achieve this goal, NCSC has identified three strategic objectives and two initiatives:

Strategic Objectives

Objective 4.1 | Strengthen Stakeholder Engagement

Lead and participate in CI and security stakeholder governance bodies to enhance transparency, consensus-building and proactive engagement on CI and security issues.

Objective 4.2 | Lead Counterintelligence and Security Policy and Strategy Development

Lead the development and implementation of the *National CI Strategy* and *UIS for CI*; drive continuous improvement through mission reviews and the state of the CI mission. Provide security and countermeasures policy guidance and advise on CI cyber, wireless, and supply chain risk management policy.

Objective 4.3 | Advance the Counterintelligence and Security Workforce

Lead the development and retention of a highly skilled, diverse, and technically capable workforce with advanced CI and security competencies.

Initiatives

Initiative 4.1 | Oversight Committee Engagement

Strengthen our responsiveness to our oversight committees. Work with the ODNI Office of Legislative Affairs to respond in a timely manner to all Congressional inquiries and taskings.

Initiative 4.2 | Governance and Advocacy

Develop combined CI and security forums, advocate for shared mission priorities and resource plans to close critical CI and security gaps and launch new initiatives.

5 Goal 5: Achieve our Mission through Organizational Excellence

Integrating CI and security capabilities finds operational and organizational efficiencies to ensure that NCSC is the nation's premier source for CI and security expertise. Improving our organizational performance at all levels requires that we build an organizational reputation defined by our hallmarks--being accessible, responsive, transparent and accountable. Reputations are vital to organizational success, and while hard to win, are easily lost. Our mission partners and stakeholders will be more willing to support our mission and goals when there is trust and communication. The scope of CI and security challenges, the broad range of our mission partners and stakeholders and the fast-paced nature of our work demands that the backbone of NCSC must remain a dedicated and highly-engaged workforce with current skills and a results-oriented outlook. To achieve this goal, NCSC has identified three strategic objectives and three initiatives:

Strategic Objectives

Objective 5.1 | NCSC Organization and Reputation

Structure NCSC to be transparent and accountable. Anticipate how NCSC must evolve to be effective. Foster an expectation that employees at all levels show leadership in their areas of responsibility and be accessible and responsive to mission partners and stakeholders.

Objective 5.2 | NCSC Workforce Development

Strengthen our professional development efforts to attract and retain a diverse and highly capable workforce that is collaborative and results-oriented.

Objective 5.3 | Strengthen NCSC Internal Processes

Provide clear direction in key management areas of human capital, facilities and infrastructure, security, information technology, program management, financial management, and contracting.

Initiatives

Initiative 5.1 | Share the Mission

Convene NCSC mission-focused events to build camaraderie and share with each other how our CI and security goals are being met. Equip our workforce to be NCSC ambassadors capable of building strong relationships with our mission partners and stakeholders.

Initiative 5.2 | Cross the Line

Facilitate and encourage employees to cross NCSC organizational lines to share the mission and work on high-priority projects for career development in the CI and security disciplines.

Initiative 5.3 | First Responders

Improve NCSC response time to all ODNI and Congressional Taskings to ensure our reputation as a responsive and accountable organization.

NCSC: Organization, Core Programs, Publications and Governance

National Intelligence Manager for Counterintelligence

Organization: National Counterintelligence Officers (NCIOs); National Counterintelligence Task Force for US; Critical Infrastructure; CI Mission Integration; CI Collection Strategy; CI Analytic Advancement.

Core Programs | Publications: *National Threat Identification and Prioritization Assessment (NTIPA); Counterintelligence Production Guidance*; *Strategic Counterintelligence Priorities*; Collection Emphasis Messages; CI Collection Assessments.

Governance: Chair: Counterintelligence Strategy Board.

Operations Coordination Directorate

Organization: Whole-of-Government Operations; Operations Support; Special Projects.

Core Programs | Publications: *Strategic Guidance for Offensive and Cyber Counterintelligence Operations; National Assessment of the Effectiveness of US Offensive Counterintelligence Operations.*

Governance: Whole-of-Government Operations Executors Working Group.

Technical and Cyber Directorate

Organization: Technical and Signals Security Countermeasures; Cyber CI and Security, NCIO for Cyber; Emerging Threats; Deputy Director IC Security Coordination Center.

Core Programs | Publications: Technical and Signal Security Modernization; IC Wireless Security Guidance; Integrated Defense of IC Information Technology Enterprise; Economic Espionage in Cyberspace.

Governance: Co-Chair, Wireless Steering Committee; Co-Chair Technical and Signal Security Executive Steering Committee.

Supply Chain Directorate

Organization: Supply Chain Threat Identification and Analysis; Supply Chain Risk Management (SCRM); SCRM Information Sharing; SCRM Education, Training and Awareness.

Core Programs | Publications: *Supply Chain Standards; SCRM Best Practices.*

Governance: Intelligence Community Supply Chain Executive Steering Group; Federal CNSS SCRM Sub-Working Group; Leading role in White House on Supply Chain; Public/Private Sector Co-Chair, Enduring Security Framework Commercial Threat Working Group.

Special Security Directorate

Organization: Personnel Security; Community Service; Continuous Evaluation.

Core Programs | Publications: Security Executive Agent (SecEA) Policies, Guidance and Oversight; Sec EA National Assessment Program (SNAP); IC Security Clearance Repository (Scattered Castles); IC Badge Reciprocity; Behavioral Analysis Research; Physical Security Programs.

Governance: IC Security Directors Board; SecEA Advisory Committee; Co-Chair, Federal Investigative Standards Implementation Working Group; Scattered Castles Executive Steering Group; Sensitive Compartmented Information Facilities (SCIF) Repository Working Group; National Security Psychology Leadership Council.

Center for Security Evaluation

Organization: US Embassy and Consulate Construction Security; Critical Threats to Overseas Facilities; Security Programs and Analysis; Technology and Information Assurance.

Core Programs | Publications: Security requirements for US Embassy and Consulate construction; Protect IC work spaces against CI threats and security vulnerabilities; Support Security Environmental Threat List; Force Protection Issues; Emerging threats against overseas IC work spaces (architectural shielding of diplomatic facilities).

Governance: Represent the IC at the Overseas Security Policy Board; Department of State Accountability Review Board Technical Requirements Steering Committee; Construction Security Review Board Technical Threat Working Group; HUMINT Threat Working Group; IC Tunneling Steering Committee and Working Group.

Mission Integration Directorate

Organization: Federal Partner Outreach; National CI and Security Policy Development; Strategic Resource Advocacy; CI and Security Workforce Talent Development and Recognition.

Core Programs | Publications: Federal Partner Engagement; *National Counterintelligence Strategy of the United States*; IC CI Mission Reviews; National Counterintelligence and Security Awards Program; CI and security awareness materials.

Governance: Counterintelligence Mission Reviews, and Resource Advocacy.

National Insider Threat Task Force

Organization: National Insider Threat Task Force.

Core Programs | Publications: *National Insider Threat Policy and Minimum Standards; Guide to Accompany the National Insider Threat Policy and Minimum Standards; Protect Your Organization from the Inside Out: Government Best Practices*; Annual Reports.

Implementing this Strategy and Measuring Progress

This Strategy constitutes NCSC's organizational performance goals for the next five years. We have defined five Strategic Goals, 16 Strategic Objectives to achieve those goals, and 14 Initiatives—some new—some continuing to kick-start the integration of CI and security. Performance measures are essential for assessing progress and providing indicators for ways to improve. Measuring progress in detail will be captured in a set of performance indicators for each initiative. Whenever possible, we will emphasize time frames, sunset strategies when necessary and define tangible outcomes. In the meantime, we can measure the general success of our endeavors by asking five broad questions for the duration of this plan:

Has NCSC

1 Led its mission partners to advance our knowledge of, and our ability to counter or disrupt, foreign and other adversarial threats as a result of our foreign threat identification and threat prioritization, our CI analytic guidance and managing CI collection requirements?

2 Strengthened the US Government's ability to protect US critical infrastructure, facilities, networks, information, and people from adversarial activities through the effective integration of CI and security, cyber and technical threat analysis, supply chain risk management, continuous evaluation, and insider threat programs?

3 Strengthened our mission partnerships with Federal Partners, the IC, our allied partners? Conducted effective outreach to the US private sector?

4 Advocated for our stakeholders to ensure they have the know-how and resources to safeguard against the scope and severity of foreign intelligence and insider threats?

5 Advanced toward our vision for NCSC as the nation's premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats?

Conclusion

NCSC will evolve and continue to improve our nation's ability to understand, disrupt and defeat threats to the US by foreign adversaries. Built on what we have already achieved, this plan charts a course for NCSC and positions us for the future. However, our ability to adapt as an organization and to find new ways of fighting the good fight against our adversaries, whose aim is to harm America—is what will make NCSC a trusted and dynamic organization.

A Chronology of the National Counterintelligence and Security Center

NATIONAL COUNTERINTELLIGENCE EXECUTIVE
UNITED STATES OF AMERICA

2002-2014

The position of the National Counterintelligence Executive was created in 2001, and the Office of the National Counterintelligence Executive (ONCIX) was established in the Counterintelligence Enhancement Act of 2002. In 2004, in accordance with the Intelligence Reform and Terrorism Prevention Act (IRPTA), ONCIX was integrated into the Office of the Director of National Intelligence (ODNI). The ODNI/Special Security Center (SSC) and the ODNI/Center for Security Evaluation (CSE) were subsequently integrated into ONCIX in 2010 to strengthen the synergies between CI and Security. SSC, renamed the Special Security Directorate (SSD) continues to focus on personnel security, serving as the Director of National Intelligence's (DNI's) lead for Security Executive Agent (SecEA) authorities, clearance reform, and continuous evaluation. ONCIX, on behalf of the DNI, along with the FBI, on behalf of the US Attorney General, provides direction and oversight of the National Insider Threat Task Force (NITTF) which was established by Executive Order 13587[17] in 2011. CSE, in consultation with the IC, supports the Department of State in executing its responsibilities to ensure the protection of classified national security information and to provide other security-related functions affecting Intelligence Community interests at US diplomatic and consular facilities abroad.[18]

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
UNITED STATES OF AMERICA

2014-2015

On 1 December 2014, the DNI designated ONCIX as the National Counterintelligence and Security Center (NCSC) to effectively integrate and align CI responsibilities of ONCIX and security mission areas under SSD and CSE, enabling the DNI to address counterintelligence and security responsibilities under a single organization. The establishment of NCSC is consistent with the DNI's authority to establish national intelligence centers to address intelligence priorities. The National Counterintelligence Executive (NCIX) also served as the Director of NCSC, and the counterintelligence authorities articulated in the CI Enhancement Act of 2002 remained in tact.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

2015-2018

On 1 December 2015, a new seal replaced the legacy ONCIX seal to represent both CI and security, and the first *NCSC Strategic Plan* was published.

In 2017, the Intelligence Authorization Act for Fiscal Year 2017 officially renamed the Office of the National Counterintelligence Executive (ONCIX) as the National Counterintelligence and Security Center (NCSC), and the National Counterintelligence Executive as the Director of the National Counterintelligence and Security Center (D/NCSC).

[17] Executive Order 13587. *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.* 7 October 2011.

[18] *Intelligence Community Directive 707*: Center for Security Evaluation. 17 October 2008.

Principles of Professional Ethics for the Intelligence Community

As members of the Intelligence Community, we conduct ourselves according to the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation. The Intelligence Community has set forth these fundamental ethical principles that unite us and distinguish us as intelligence professionals:

Mission

We serve the American people, and understand that our mission requires selfless dedication to the security of our nation.

Truth

We seek the truth; speak truth to power; and obtain, analyze and provide intelligence objectively.

Lawfulness

We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

Integrity

We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

Stewardship

We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

Excellence

We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

Diversity

We embrace the diversity of our nation, promote diversity and inclusion in our workforce, and encourage diversity in our thinking.

NCSC

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE